

Network in the Cloud: a Map-and-Encap Approach

Damien Saucez

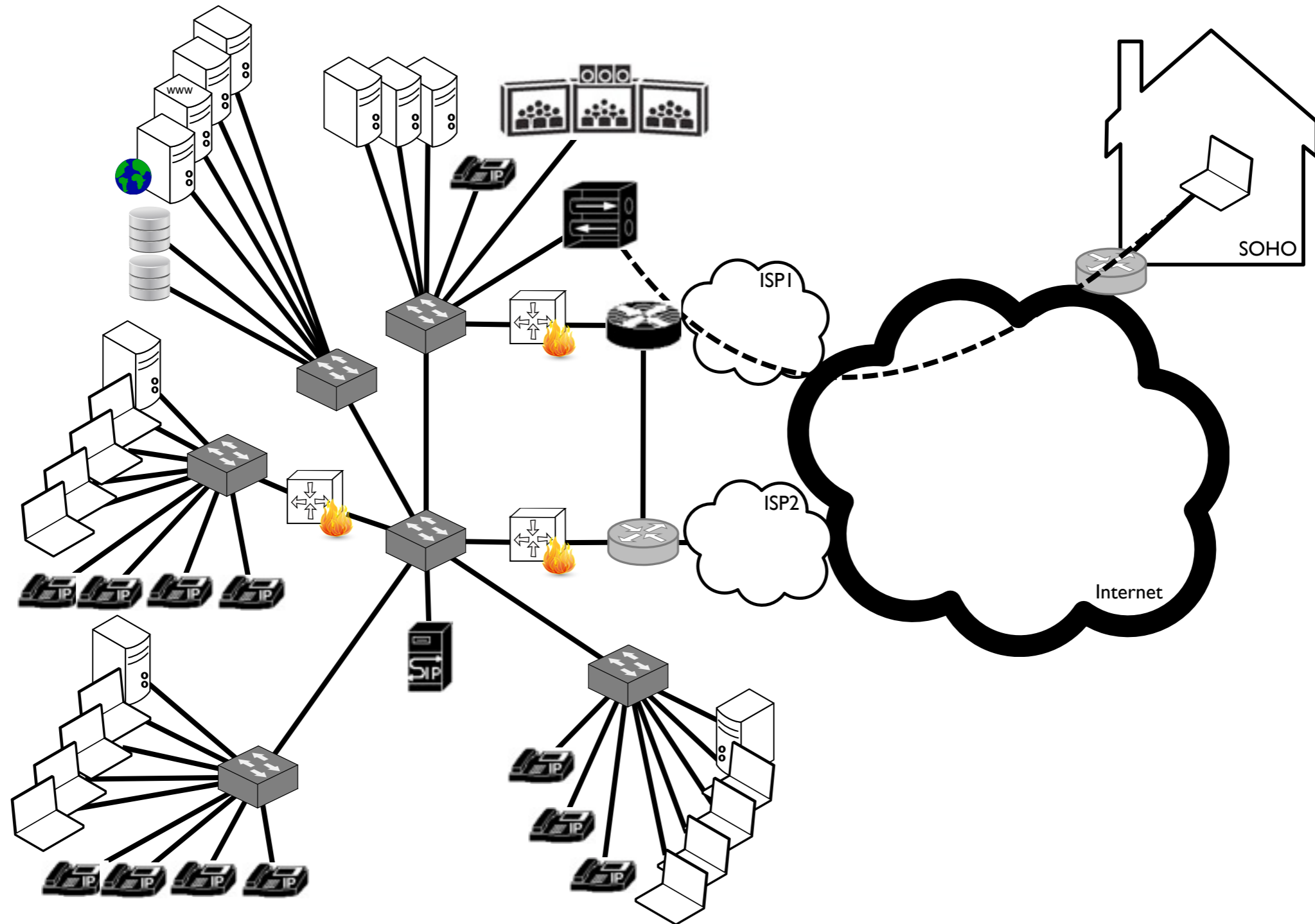
Inria

Wassim Haddad

Ericsson

IEEE CloudNet'12

Enterprise network



Enterprise network (contd.)

- Survey on 57 enterprise networks

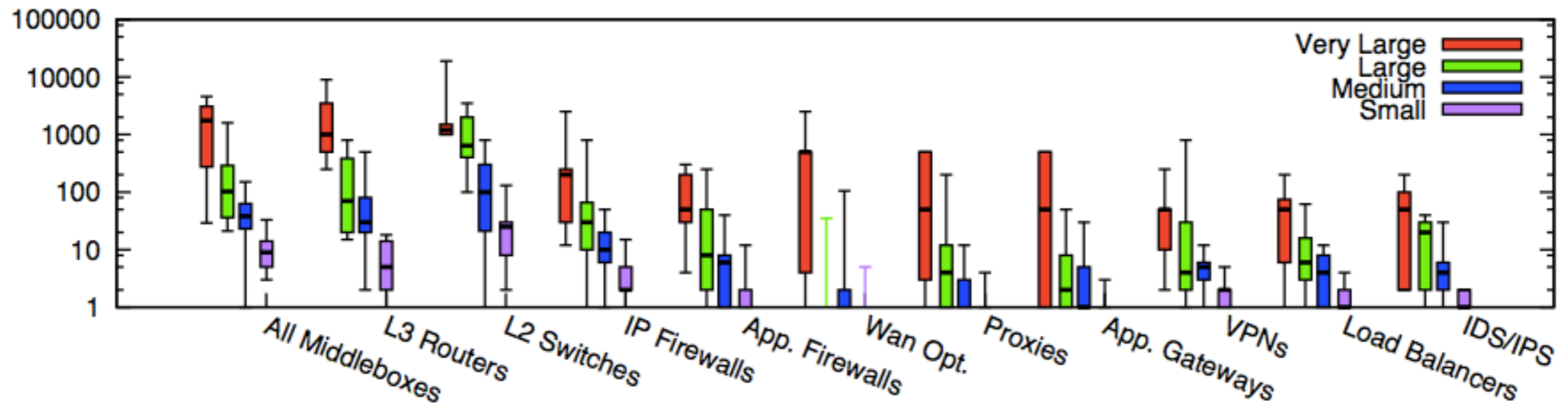


Figure 1: Box plot of middlebox deployments for small (fewer than 1k hosts), medium (1k-10k hosts), large (10k-100k hosts), and very large (more than 100k hosts) enterprise networks. Y-axis is in log scale.

Motivation

- Observation: digital communications are essential for enterprises
- Problem: fast, secure, and reliable Internet connectivity is expensive
 - high OPEX
 - high CAPEX
- Solution: outsource network operations and services to reduce costs supported by enterprises

Why not moving the infrastructure in the Cloud?

- The concept exists [1, 19], some call it Network-as-a-Services...
- NaaS gives tenants access to network infrastructure in the Cloud to implement custom forwarding decisions [1]
- ... but the lack of a simple and cheap technology to redirect traffic to the Cloud limits its deployment

Requirements for a NaaS-enabler protocol

- We need a protocol able to divert packets to/from NaaS providers that
 - has unified control-plane and data-plane
 - is available in today's equipment
 - can be deployed in the current Internet
 - has simple of maintenance and operation
 - can support highly dynamic changes
- APLOMB [19] could do it, but relies on “home made” protocol
- LISP is the perfect protocol candidate
 - relies on the map-and-encap principle

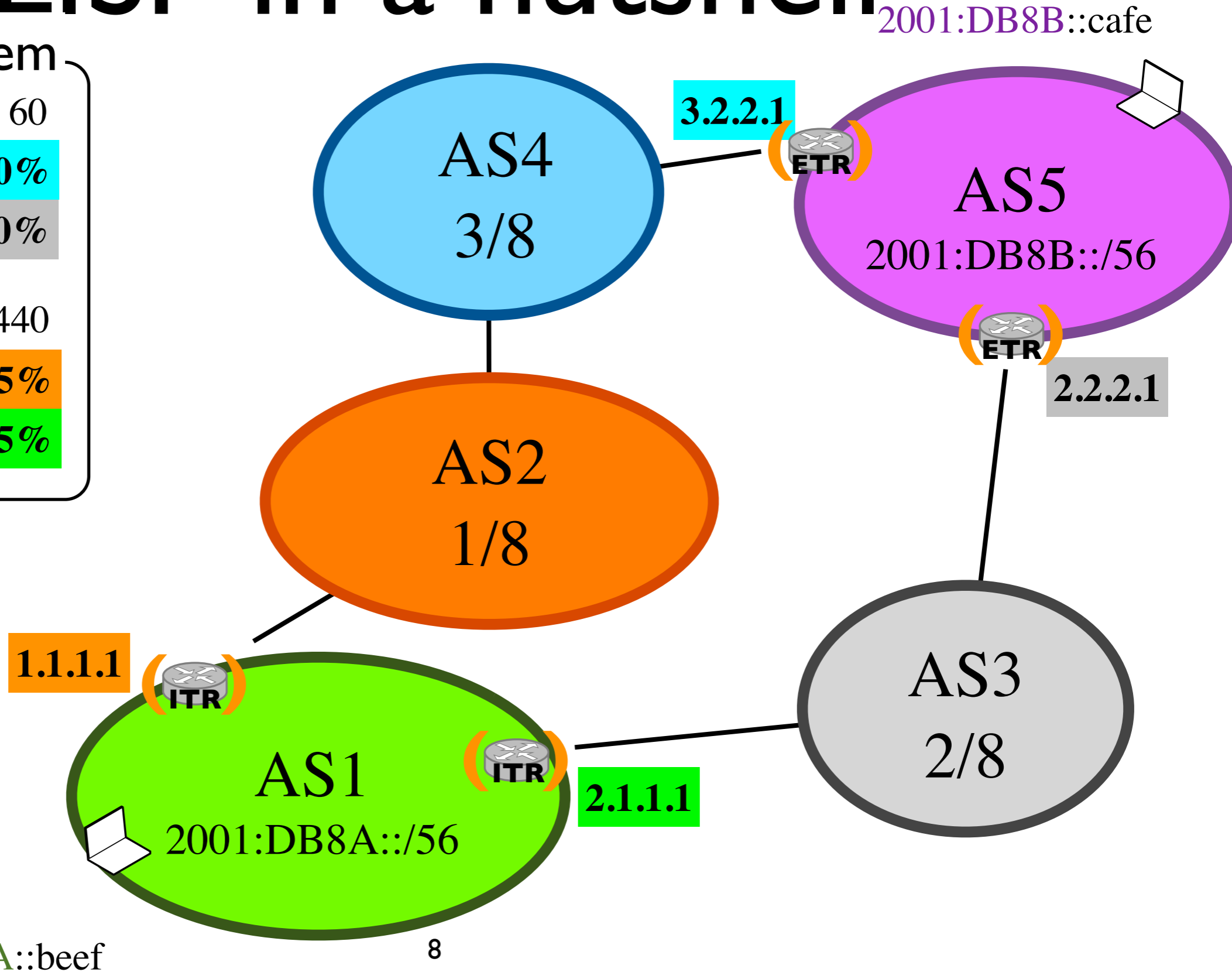
Locator/Identifier Separation Protocol (LISP)

- Split the IP address space in two at the border routers
- Endpoint IDentifiers (EID)
 - identify end-systems and edge routers
 - non-globally routable
 - end systems in a site share the same EID prefix
- Routing LOCators (RLOC)
 - attached to core routers (router interfaces)
 - globally routable
- Use Map-and-Encap to glue the two spaces

LISP in a nutshell

Mapping System

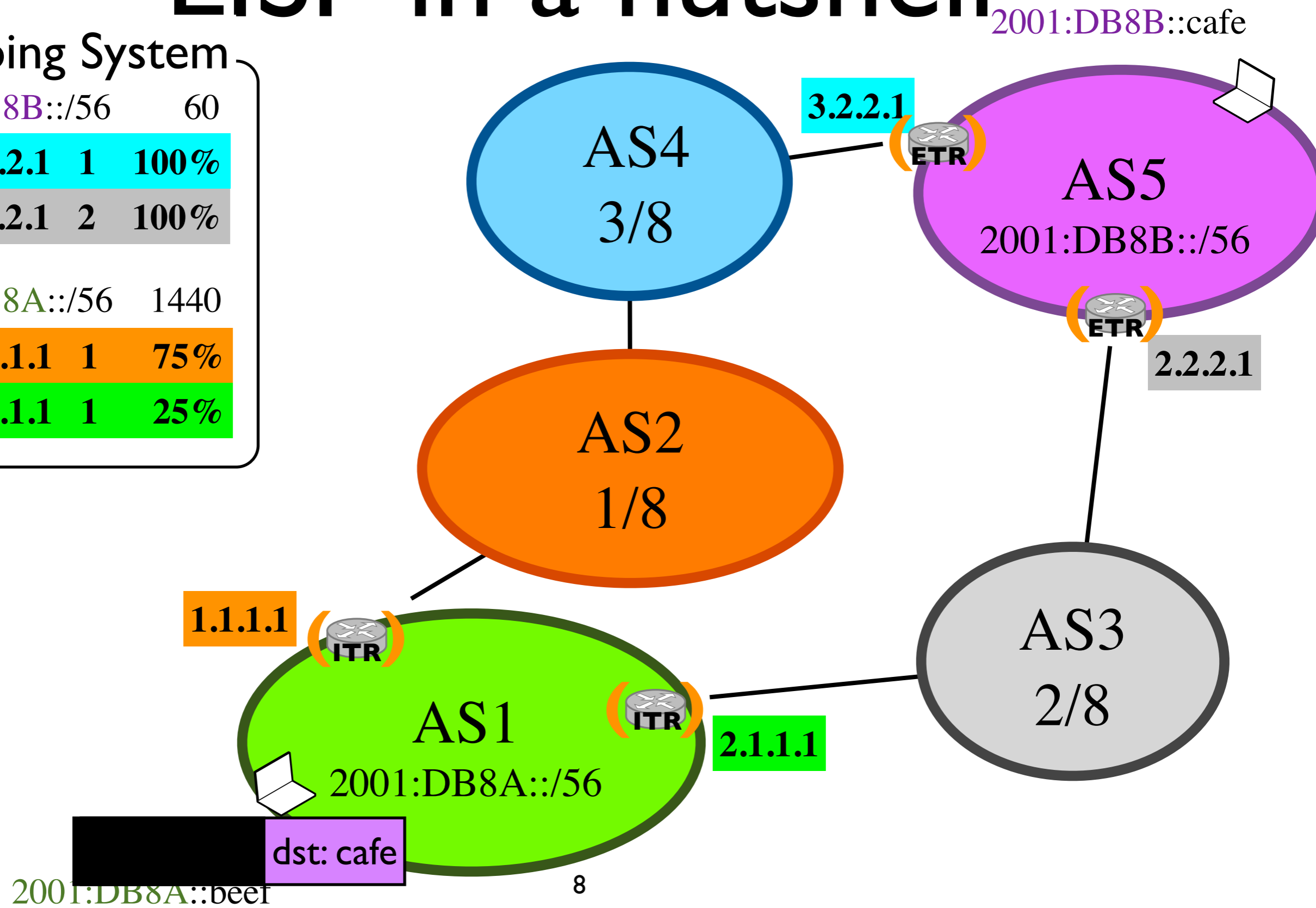
2001:DB8B:: 56</td <td>60</td>	60
3.2.2.1	1 100%
2.2.2.1	2 100%
2001:DB8A:: 56</td <td>1440</td>	1440
1.1.1.1	1 75%
2.1.1.1	1 25%



LISP in a nutshell

Mapping System

2001:DB8B::/56	60
3.2.2.1	1 100%
2.2.2.1	2 100%
2001:DB8A::/56	1440
1.1.1.1	1 75%
2.1.1.1	1 25%

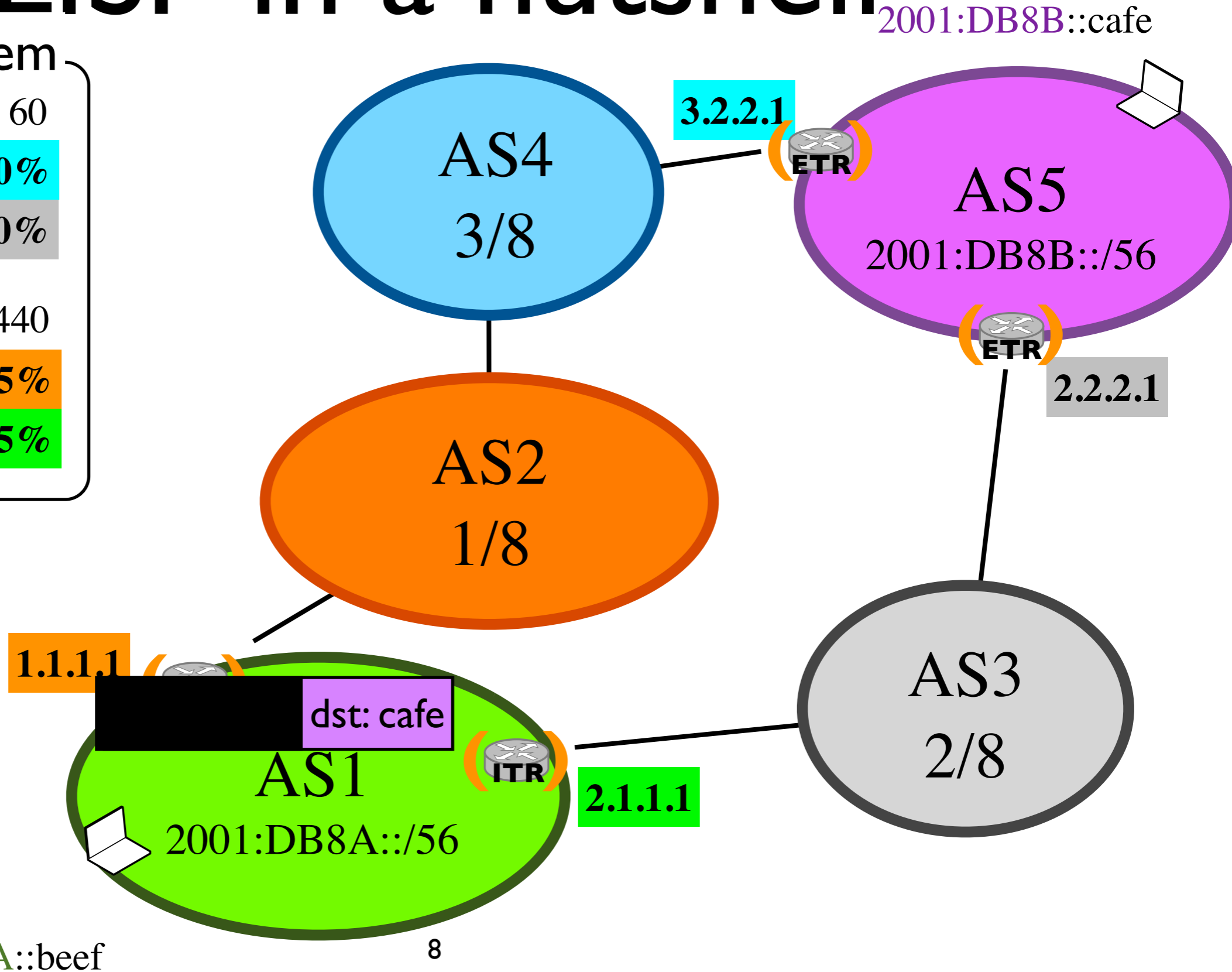


2001:DB8A::beef

LISP in a nutshell

Mapping System

2001:DB8B:: 56</td <td>60</td>	60
3.2.2.1	1 100%
2.2.2.1	2 100%
2001:DB8A:: 56</td <td>1440</td>	1440
1.1.1.1	1 75%
2.1.1.1	1 25%

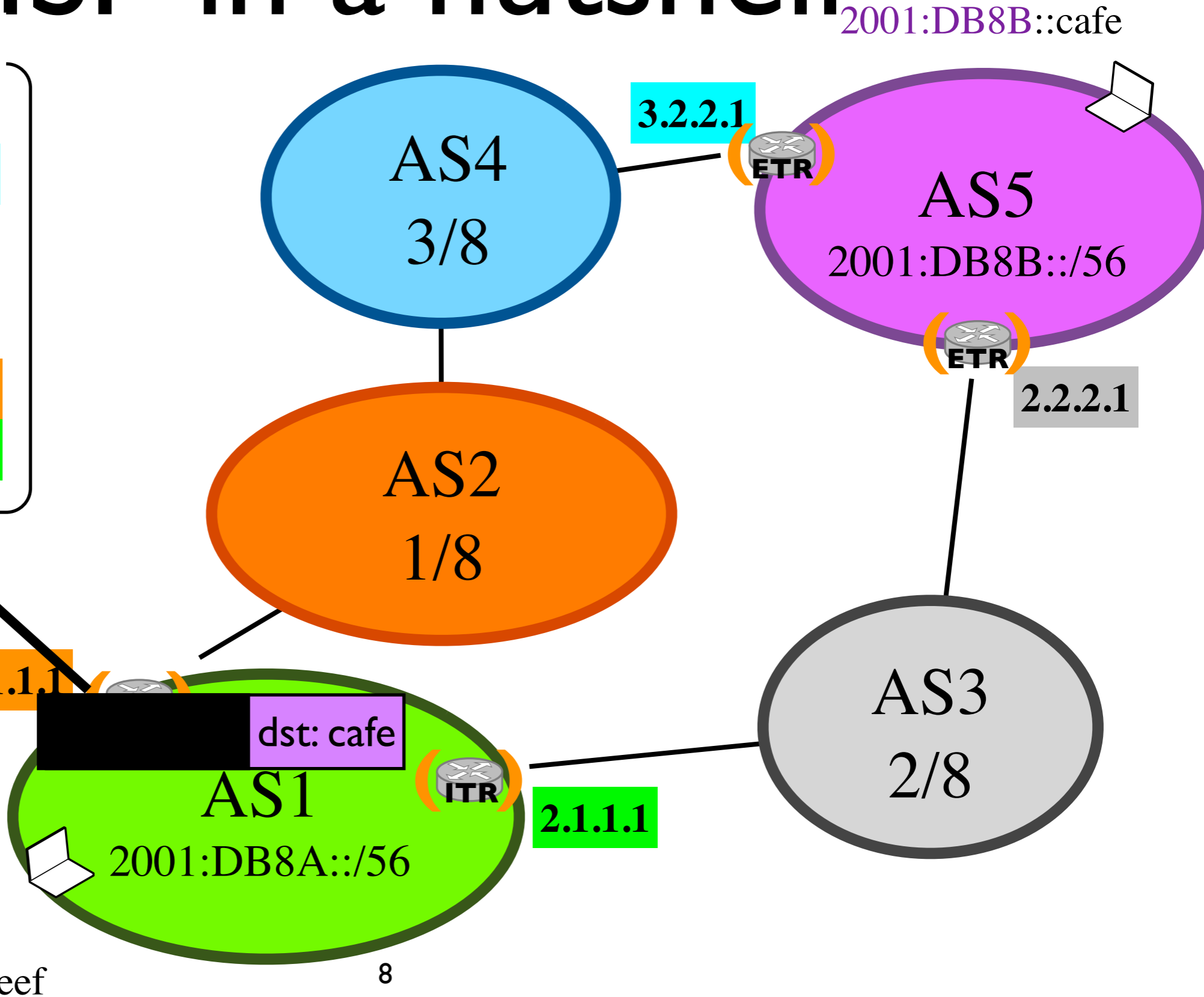


LISP in a nutshell

Mapping System

2001:DB8B:: 56</td <td>60</td>	60
3.2.2.1	1 100%
2.2.2.1	2 100%
2001:DB8A:: 56</td <td>1440</td>	1440
1.1.1.1	1 75%
2.1.1.1	1 25%

Map-Request: 1.1.1.1
 2001:DB8B::cafe?



LISP in a nutshell

Mapping System

2001:DB8B:: 56</td <td>60</td>	60
3.2.2.1	1 100%
2.2.2.1	2 100%
2001:DB8A:: 56</td <td>1440</td>	1440
1.1.1.1	1 75%
2.1.1.1	1 25%

Map-Reply:

2001:DB8B::

3.2.2.1	1 100%
2.2.2.1	2 100%

1.1.1.1

dst: cafe

AS1

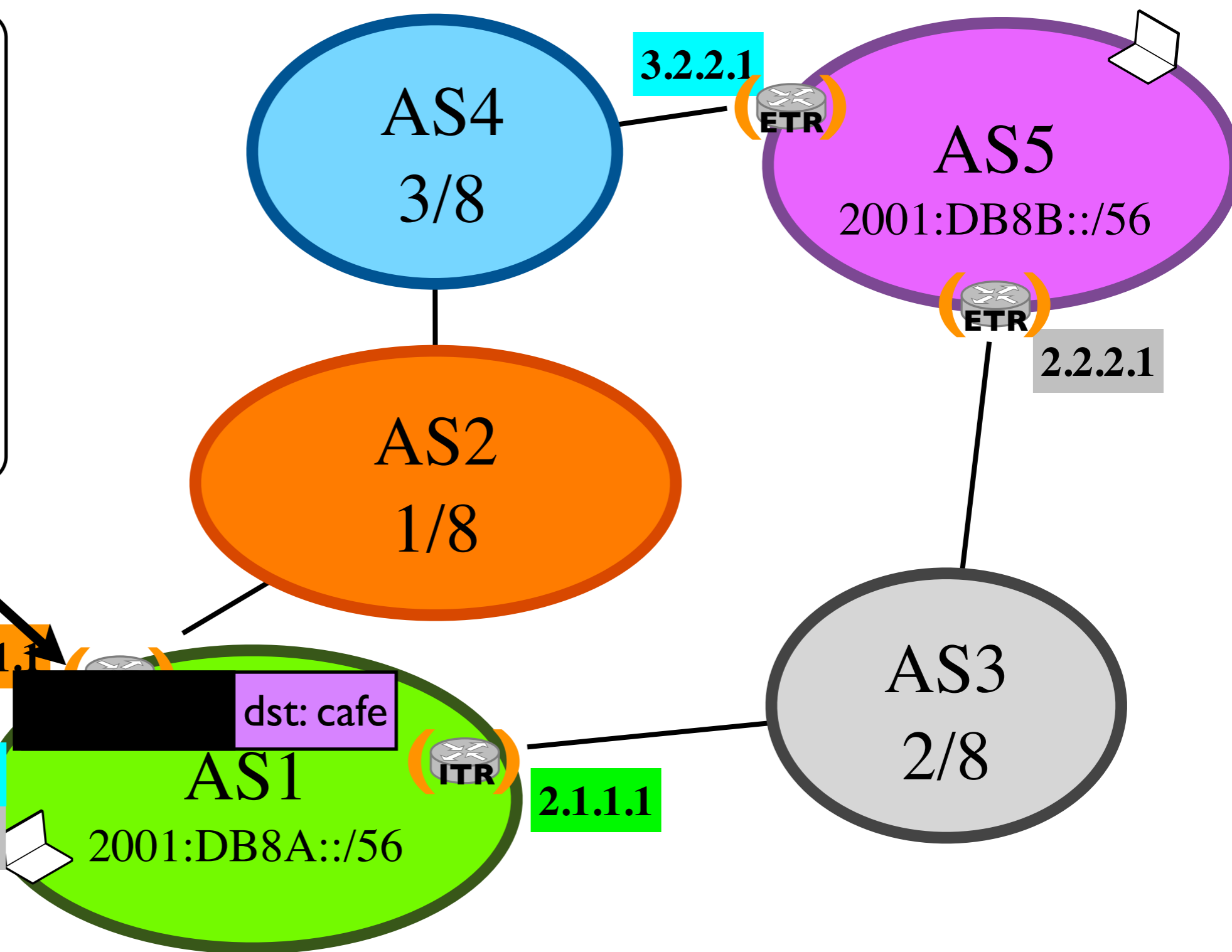
2001:DB8A::

2.1.1.1

2001:DB8A::

8

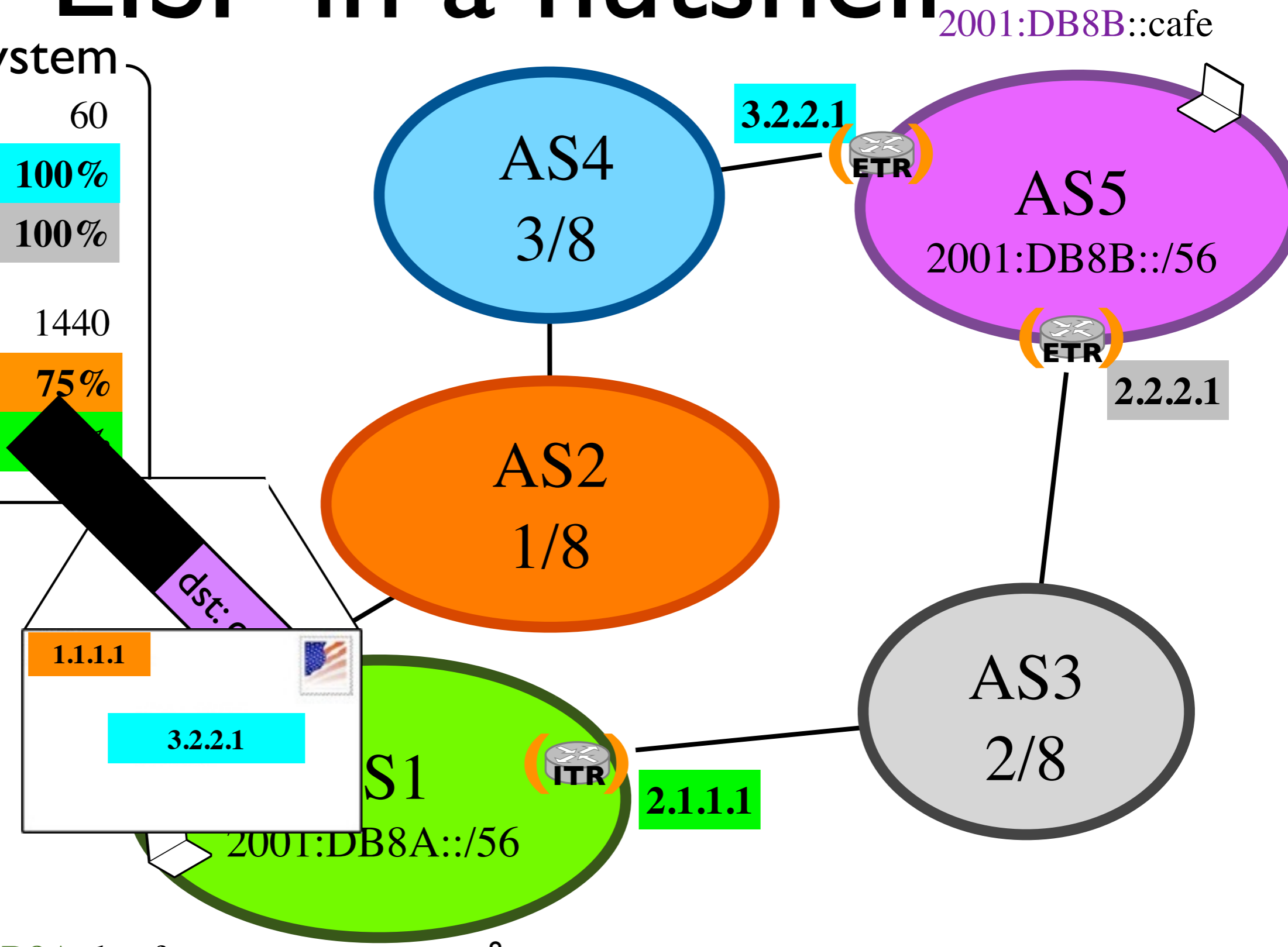
2001:DB8B::



LISP in a nutshell

Mapping System

2001:DB8B::/56	60
3.2.2.1	1 100%
2.2.2.1	2 100%
2001:DB8A::/56	1440
1.1.1.1	1 75%
2.1.1.1	1 100%

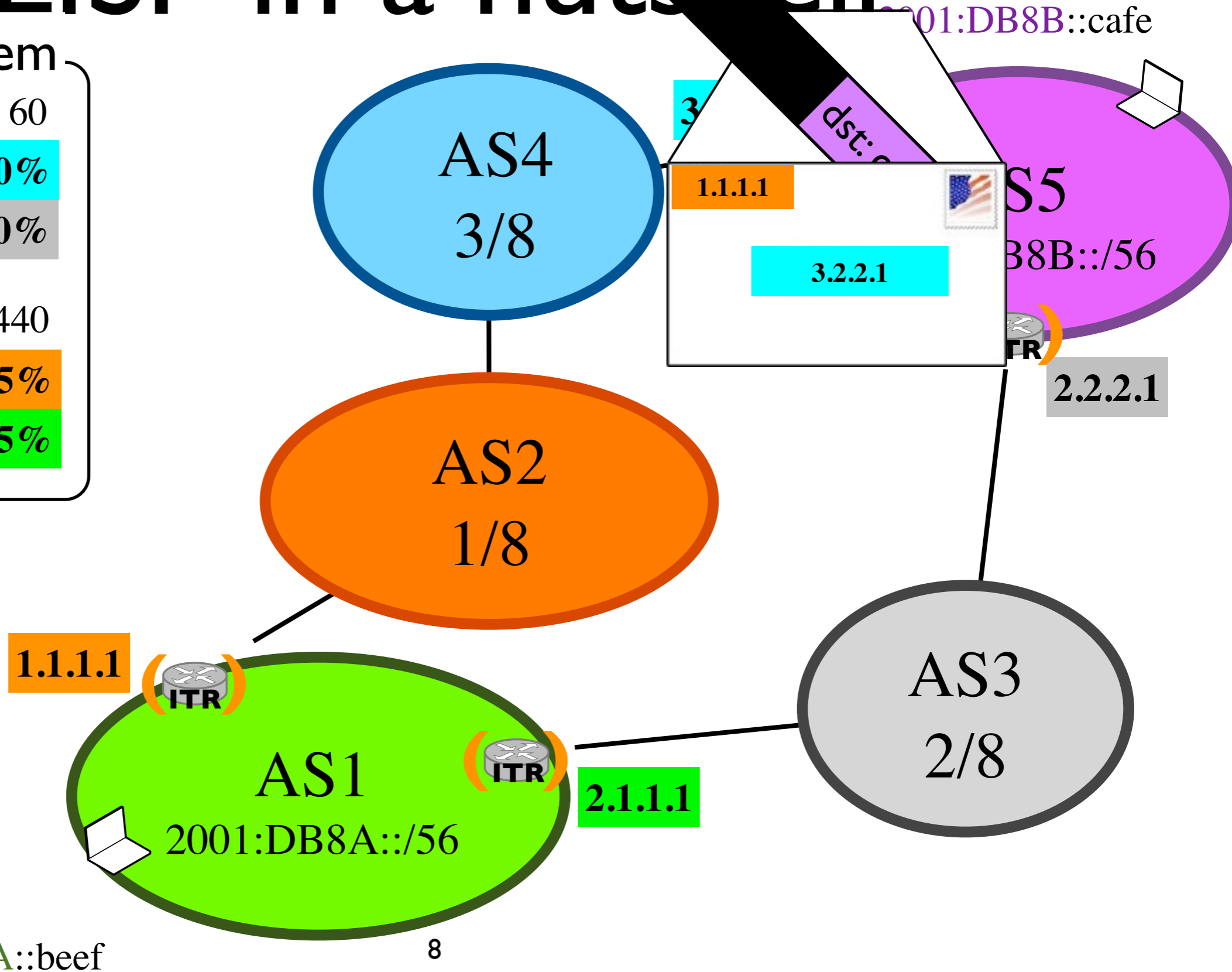


2001:DB8A::beef

LISP in a nutshell

Mapping System

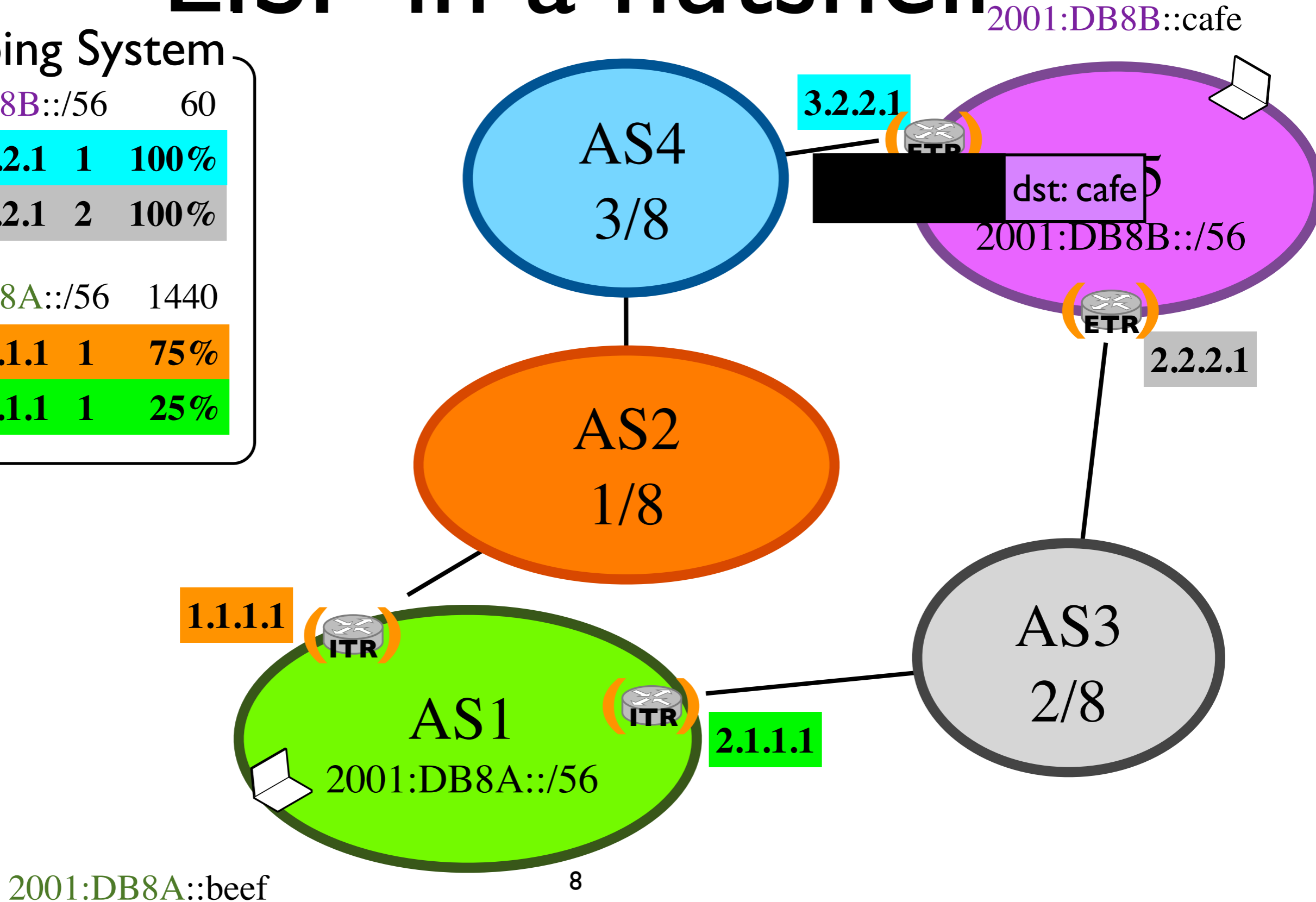
2001:DB8B:: 56</td <td>60</td>	60
3.2.2.1	1 100%
2.2.2.1	2 100%
2001:DB8A:: 56</td <td>1440</td>	1440
1.1.1.1	1 75%
2.1.1.1	1 25%



LISP in a nutshell

Mapping System

2001:DB8B:: 56</td <td>60</td>	60
3.2.2.1 1	100%
2.2.2.1 2	100%
2001:DB8A:: 56</td <td>1440</td>	1440
1.1.1.1 1	75%
2.1.1.1 1	25%

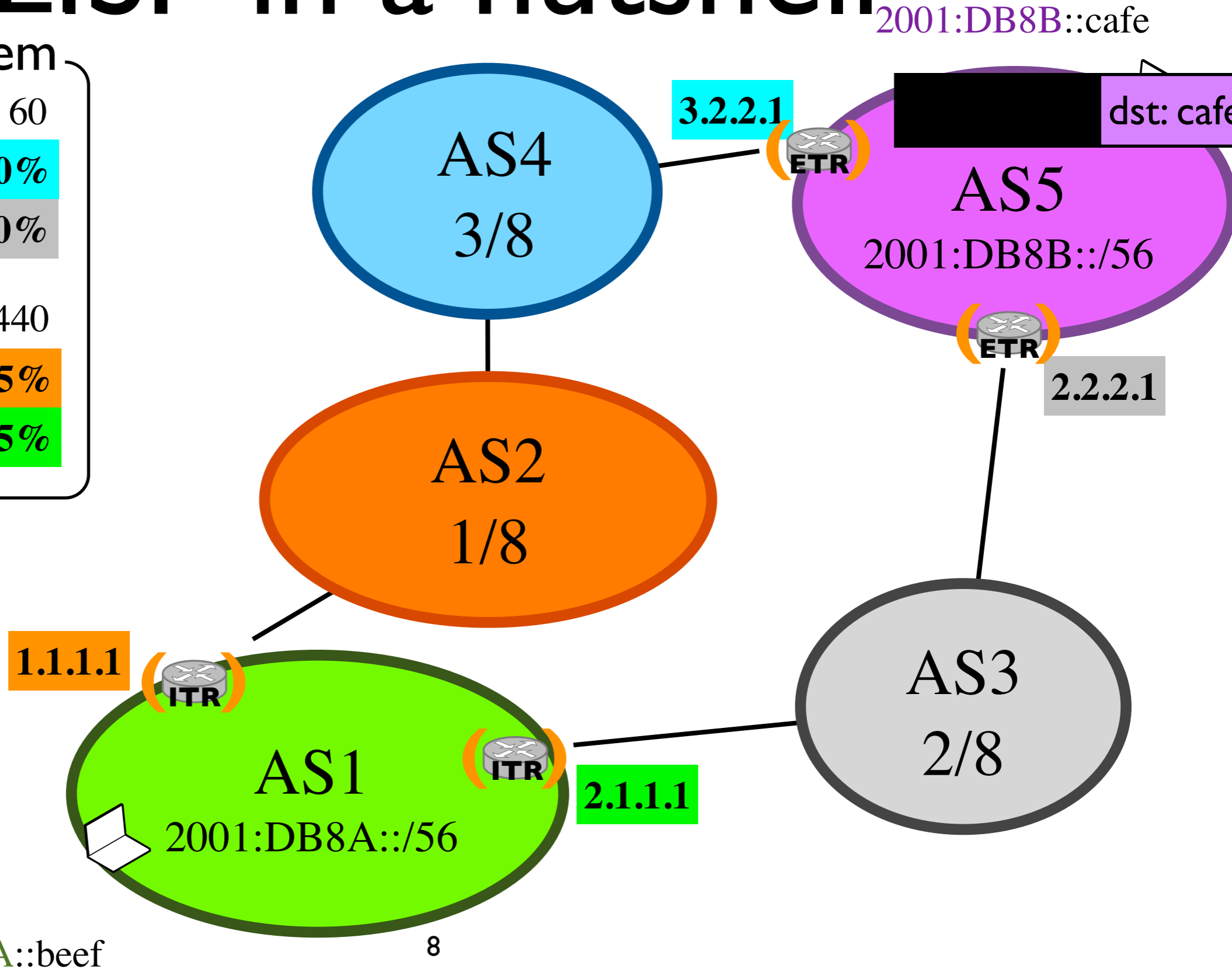


2001:DB8A::beef

LISP in a nutshell

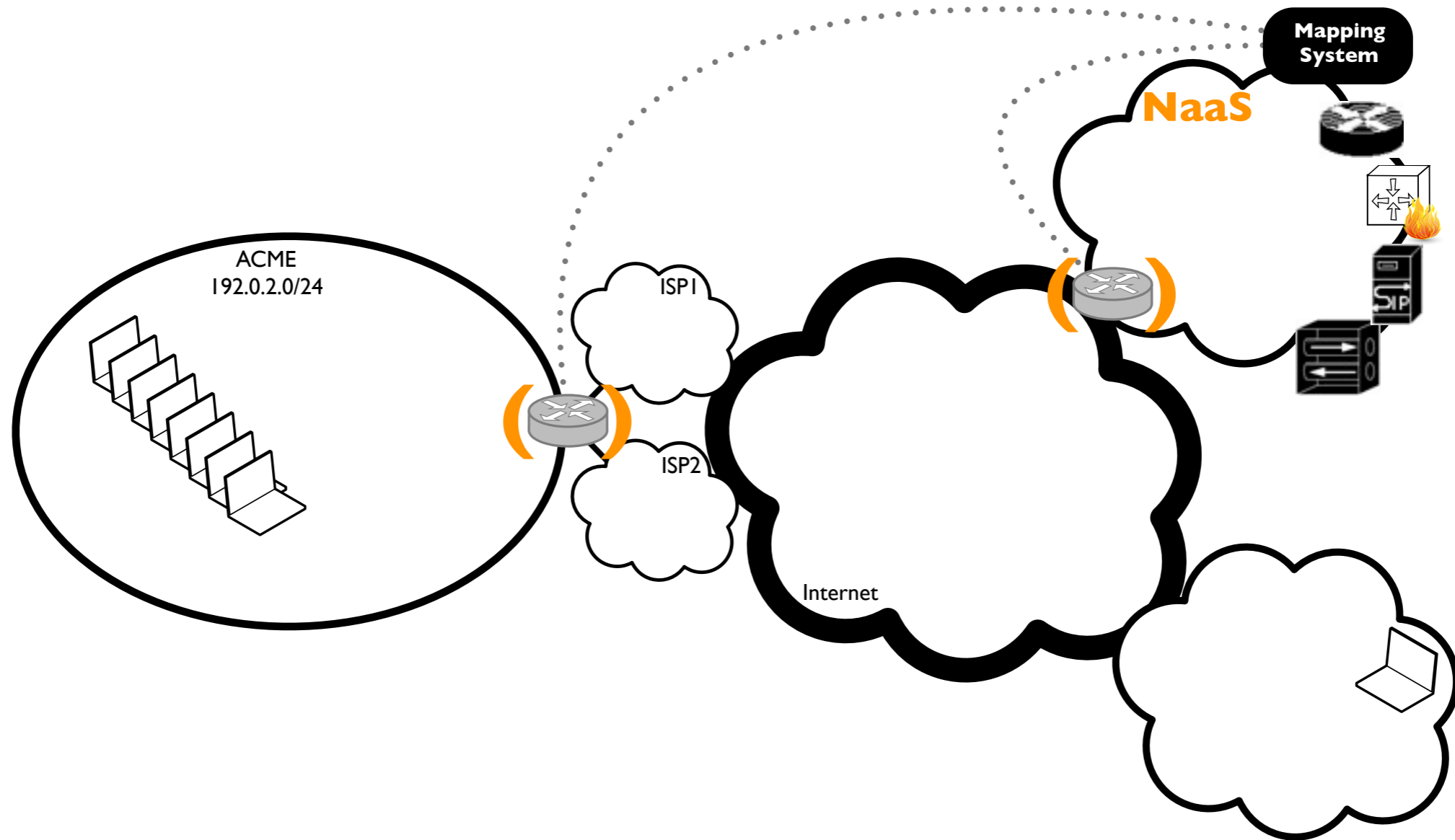
Mapping System

2001:DB8B:: 56</td <td>60</td>	60
3.2.2.1	1 100%
2.2.2.1	2 100%
2001:DB8A:: 56</td <td>1440</td>	1440
1.1.1.1	1 75%
2.1.1.1	1 25%



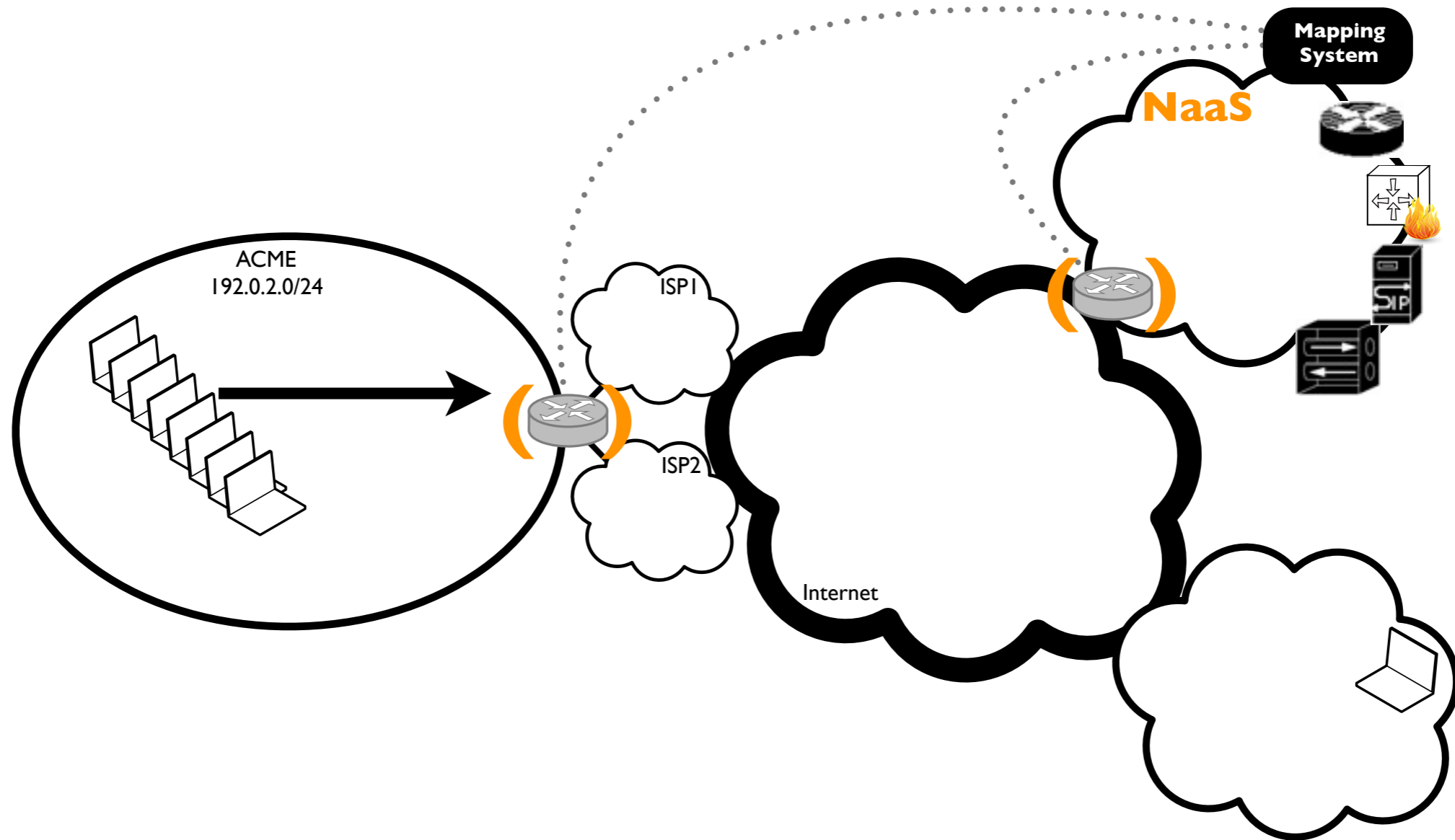
Moving packets in the Cloud with LISP

To the Internet



- Native IP forwarding
- ⋯ BGP advertisement
- - - → LISP tunnel
- () LISP router

To the Internet



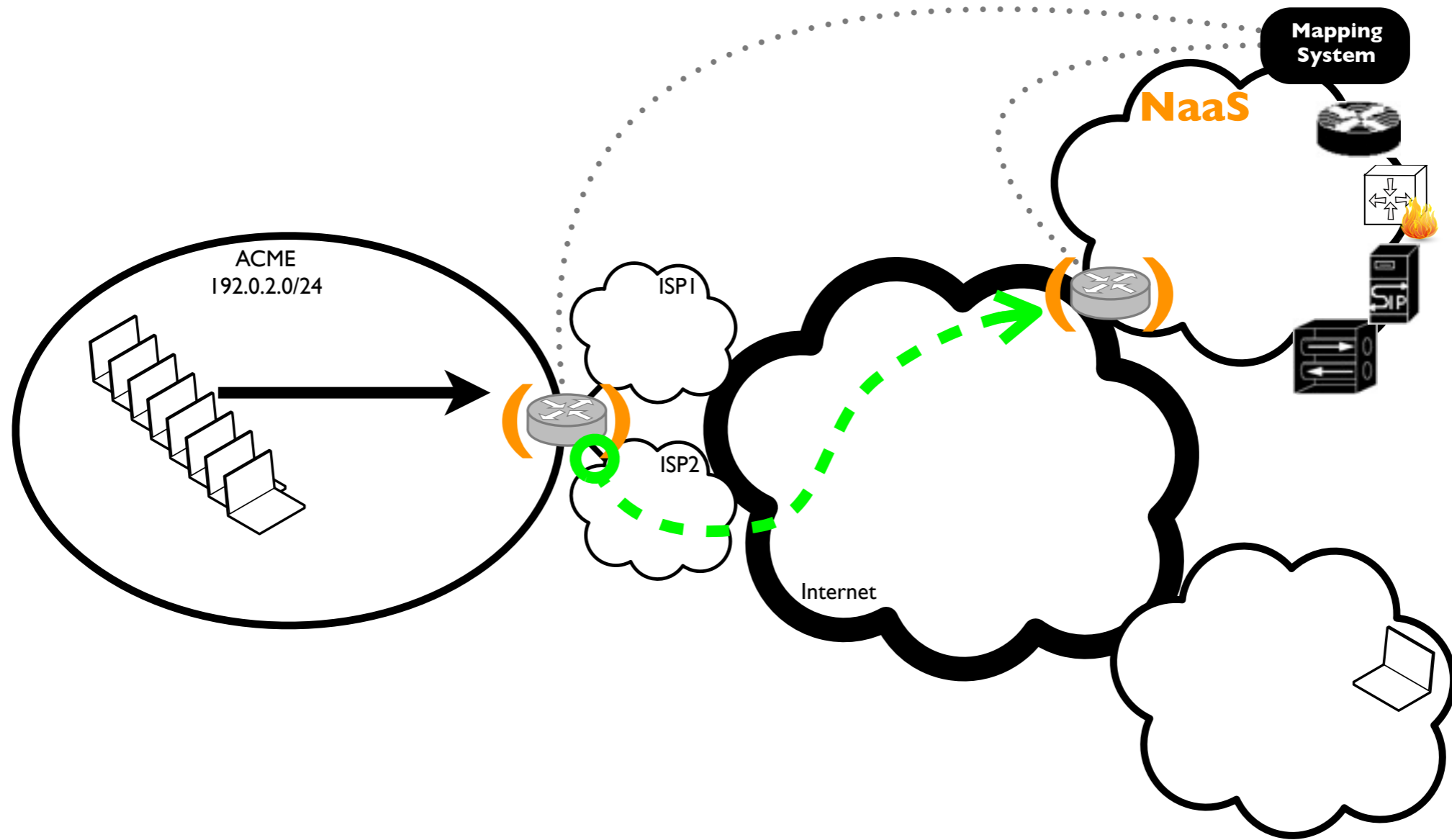
————→ Native IP forwarding

.....▶ BGP advertisement

○- - - - -▶ LISP tunnel

(Router icon) LISP router

To the Internet



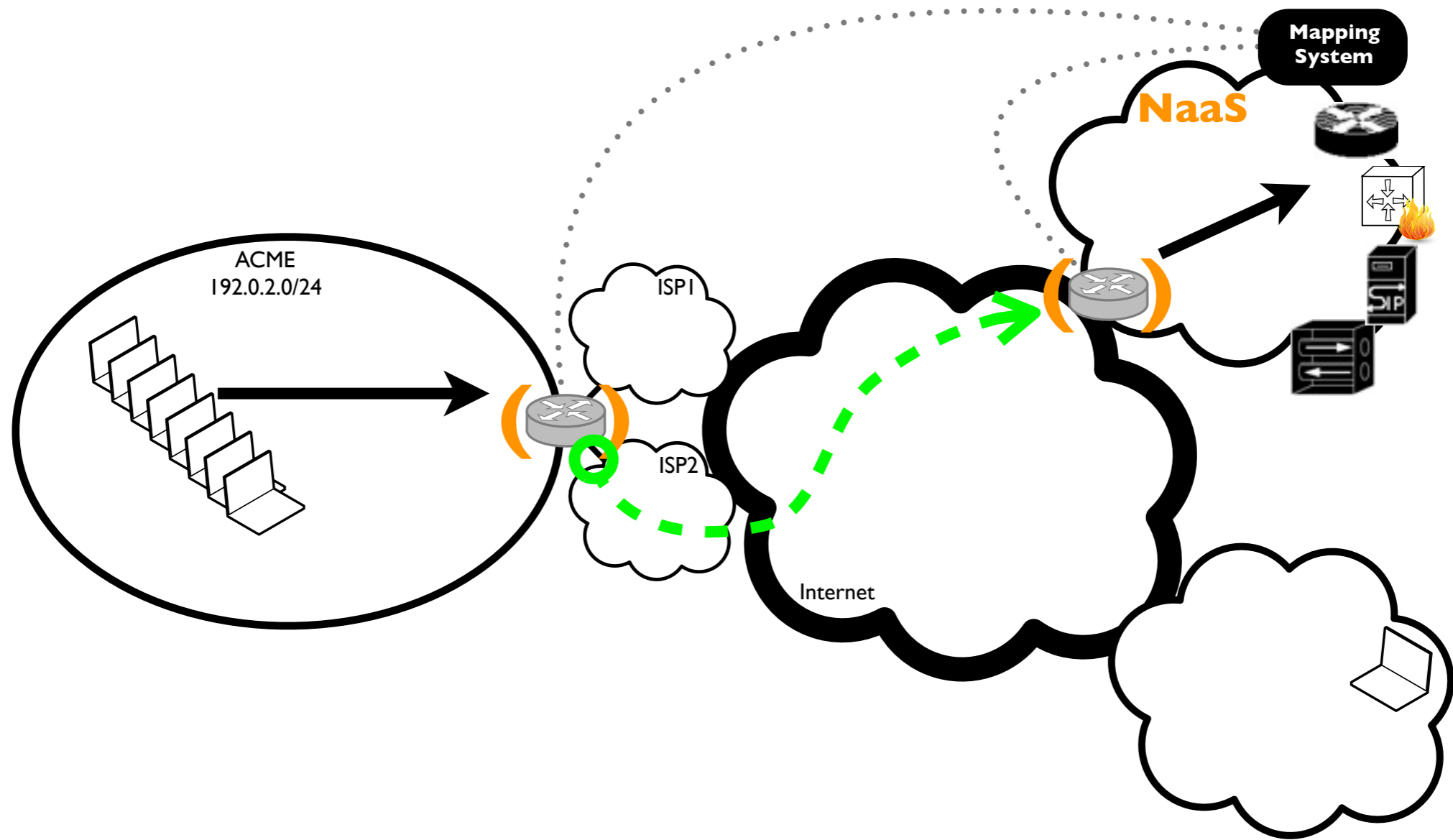
————> Native IP forwarding

○- - - -> LISP tunnel

.....▶ BGP advertisement

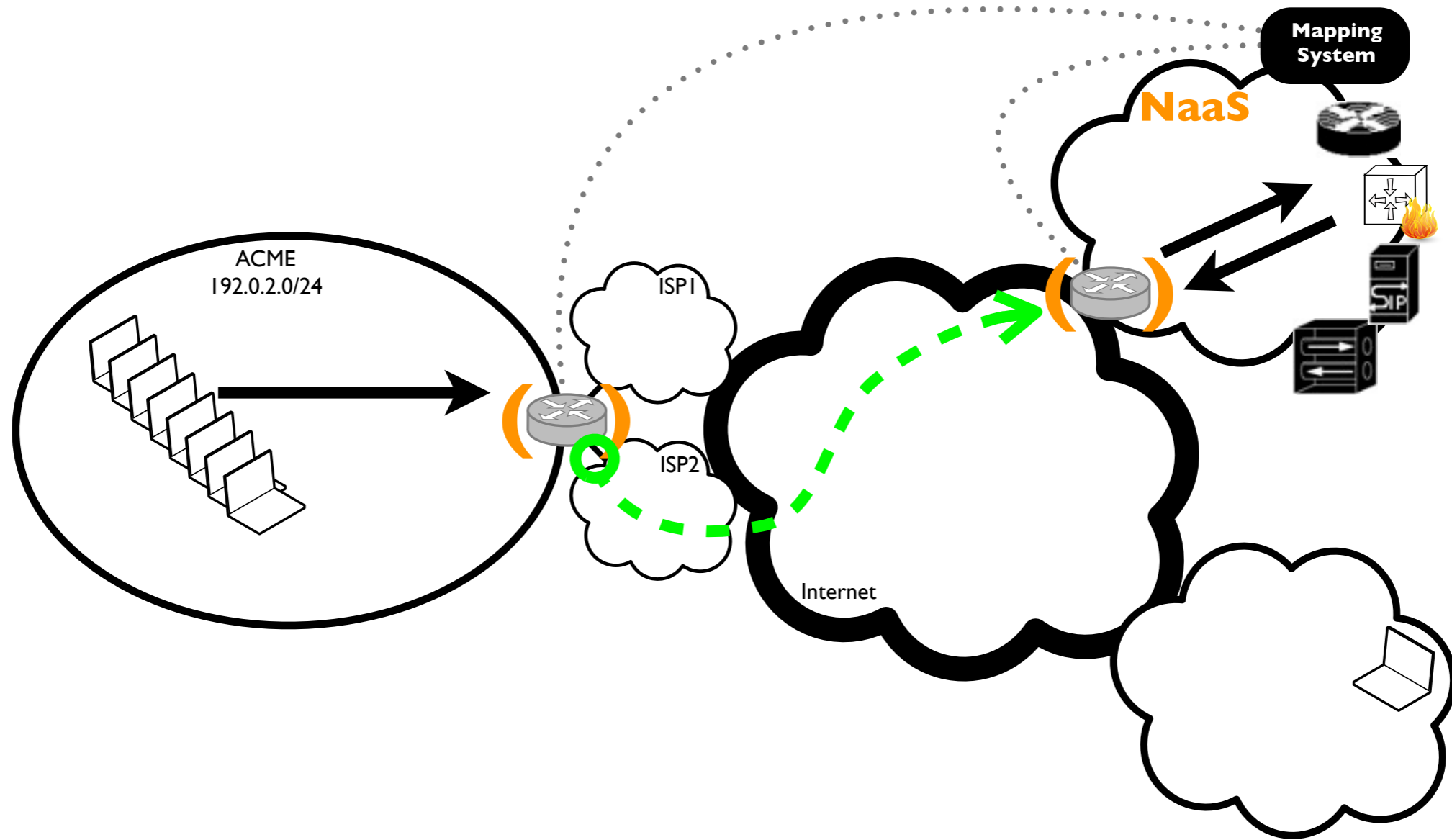
(Router icon) LISP router

To the Internet



- Native IP forwarding
- - - → LISP tunnel
-▶ BGP advertisement
- (Router icon) LISP router

To the Internet



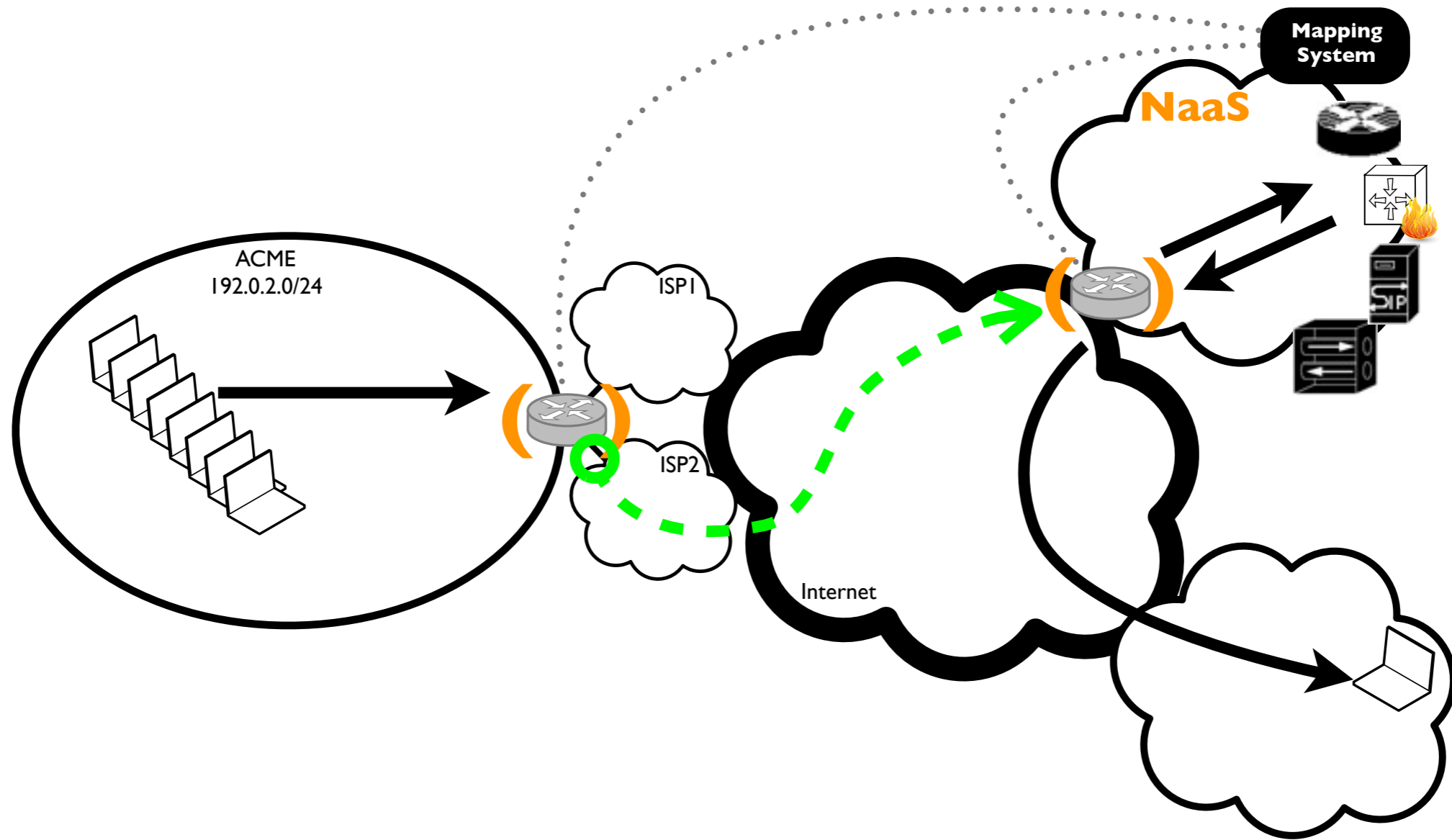
————> Native IP forwarding

○- - - -> LISP tunnel

.....▶ BGP advertisement

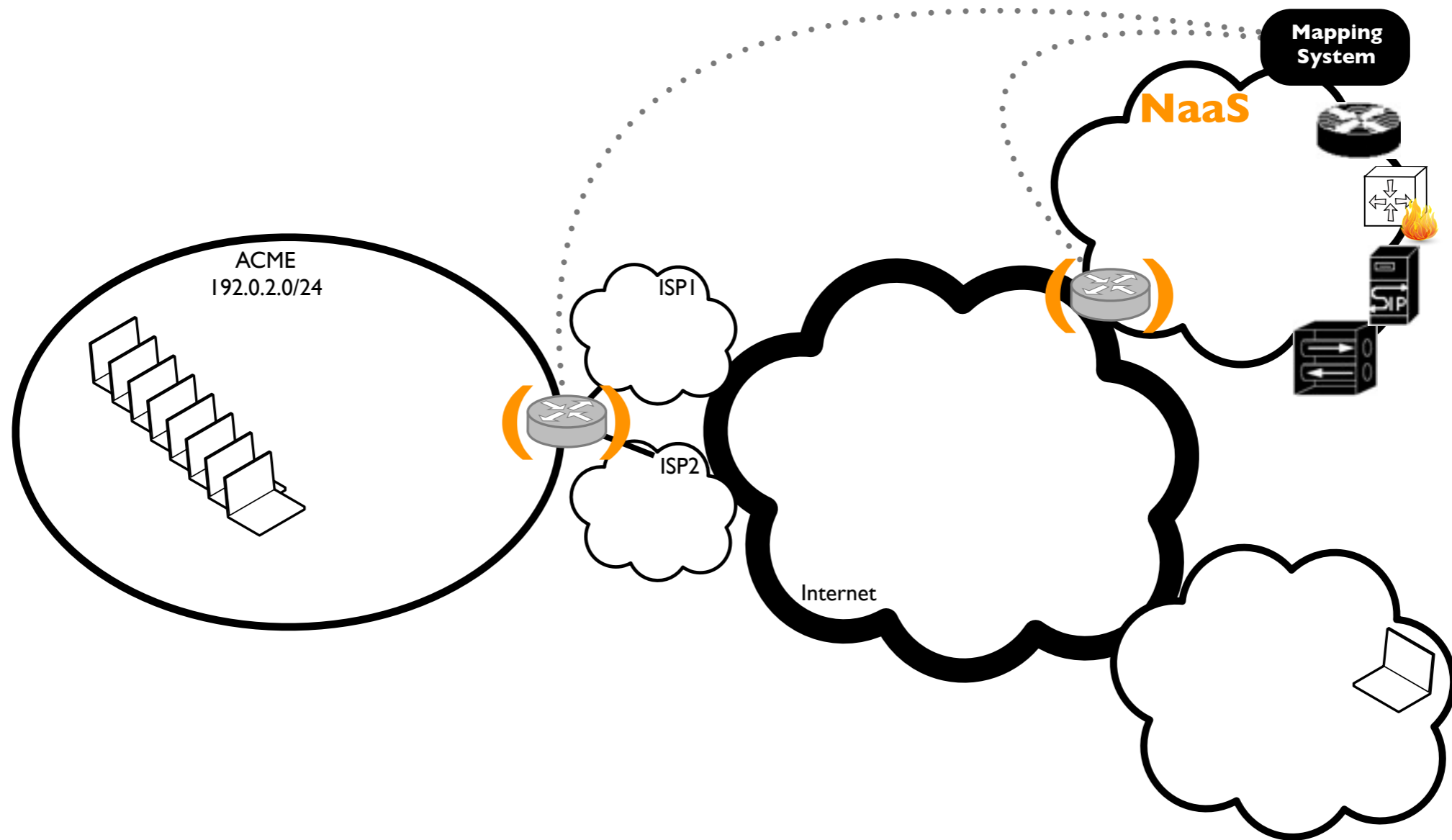
((router icon)) LISP router

To the Internet



- Native IP forwarding
-▶ BGP advertisement
- - - -> LISP tunnel
- (Router icon) LISP router

From the Internet



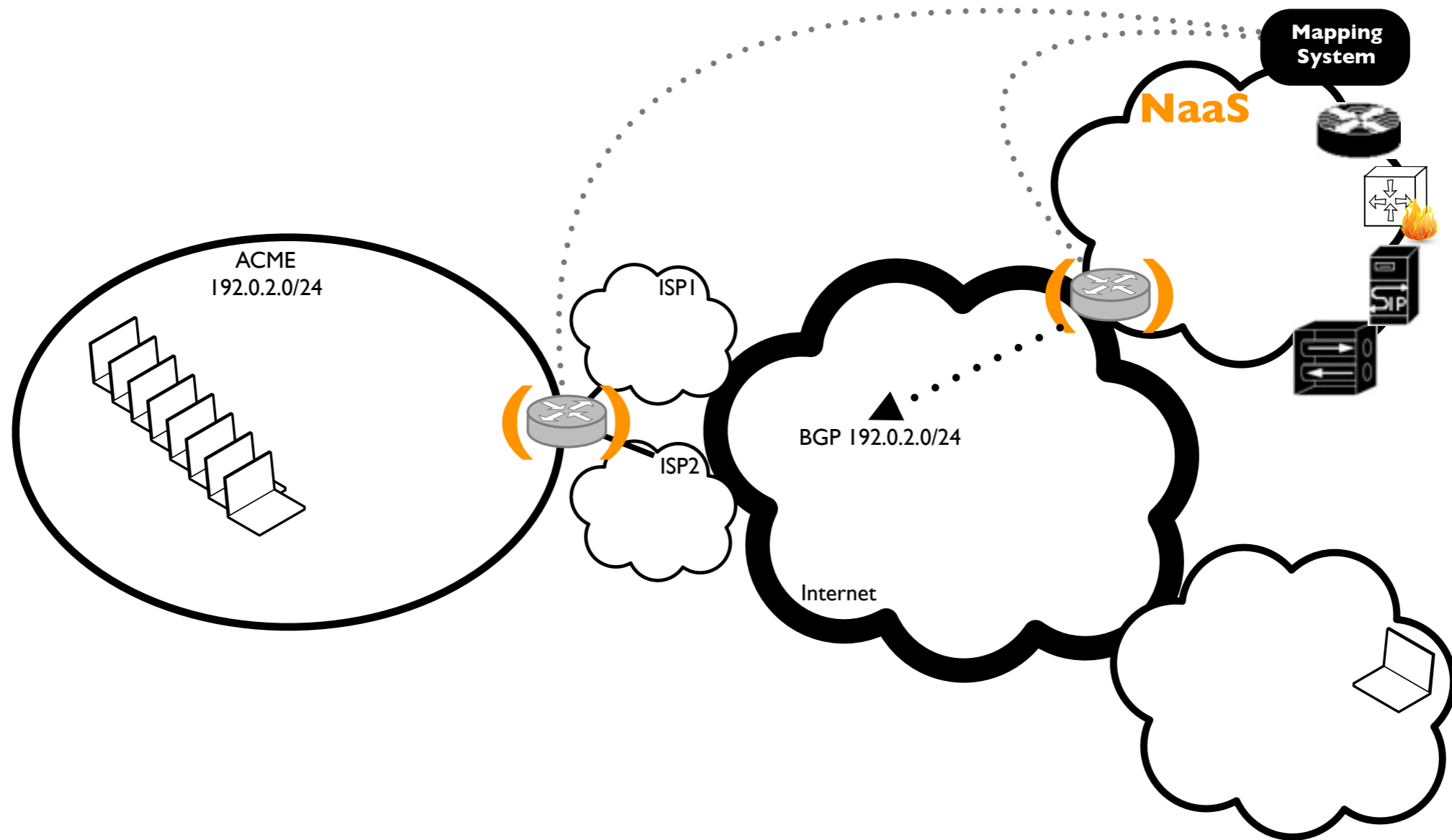
————> Native IP forwarding

○- - - -> LISP tunnel

.....▶ BGP advertisement

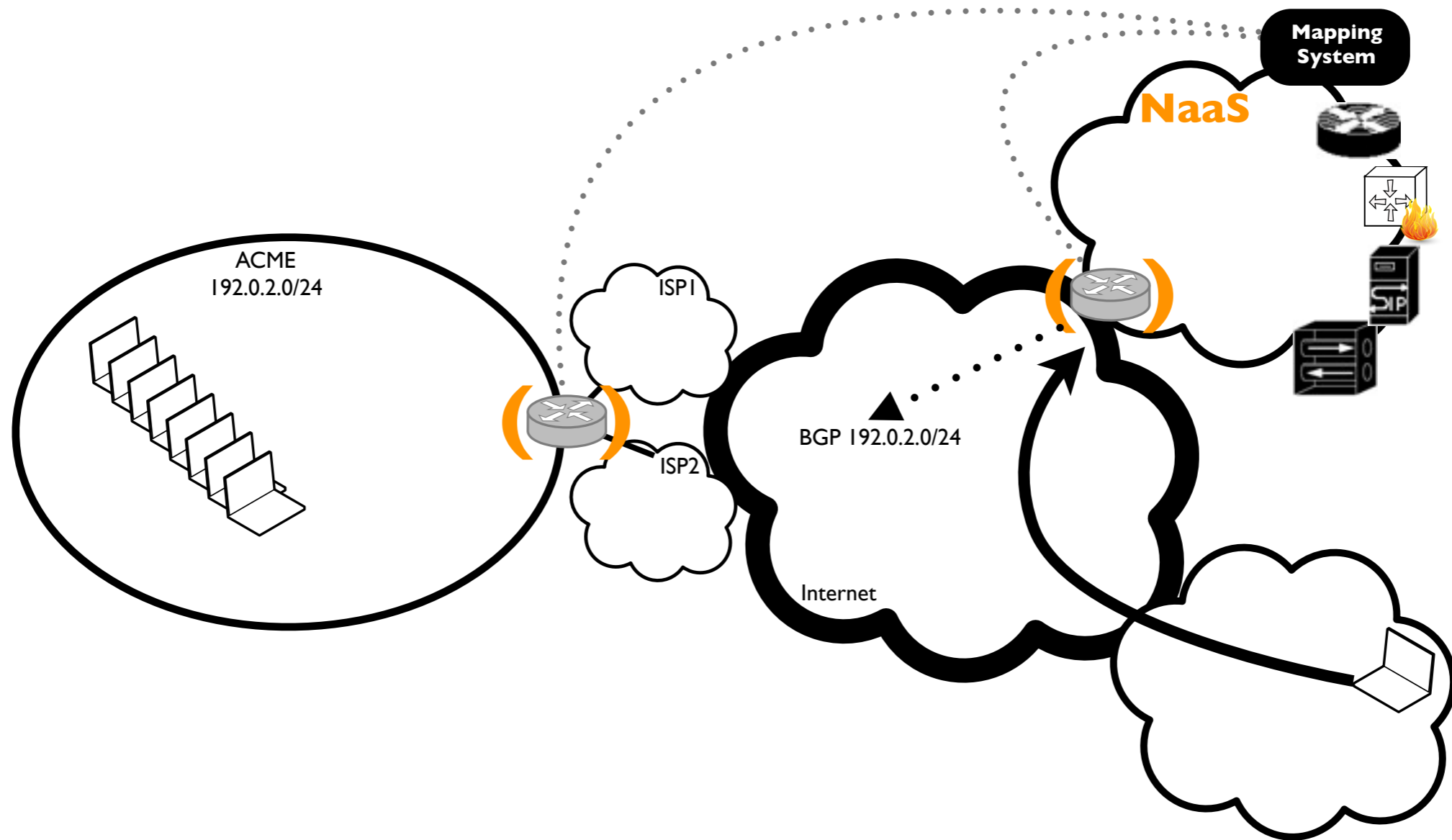
(Router icon) LISP router

From the Internet



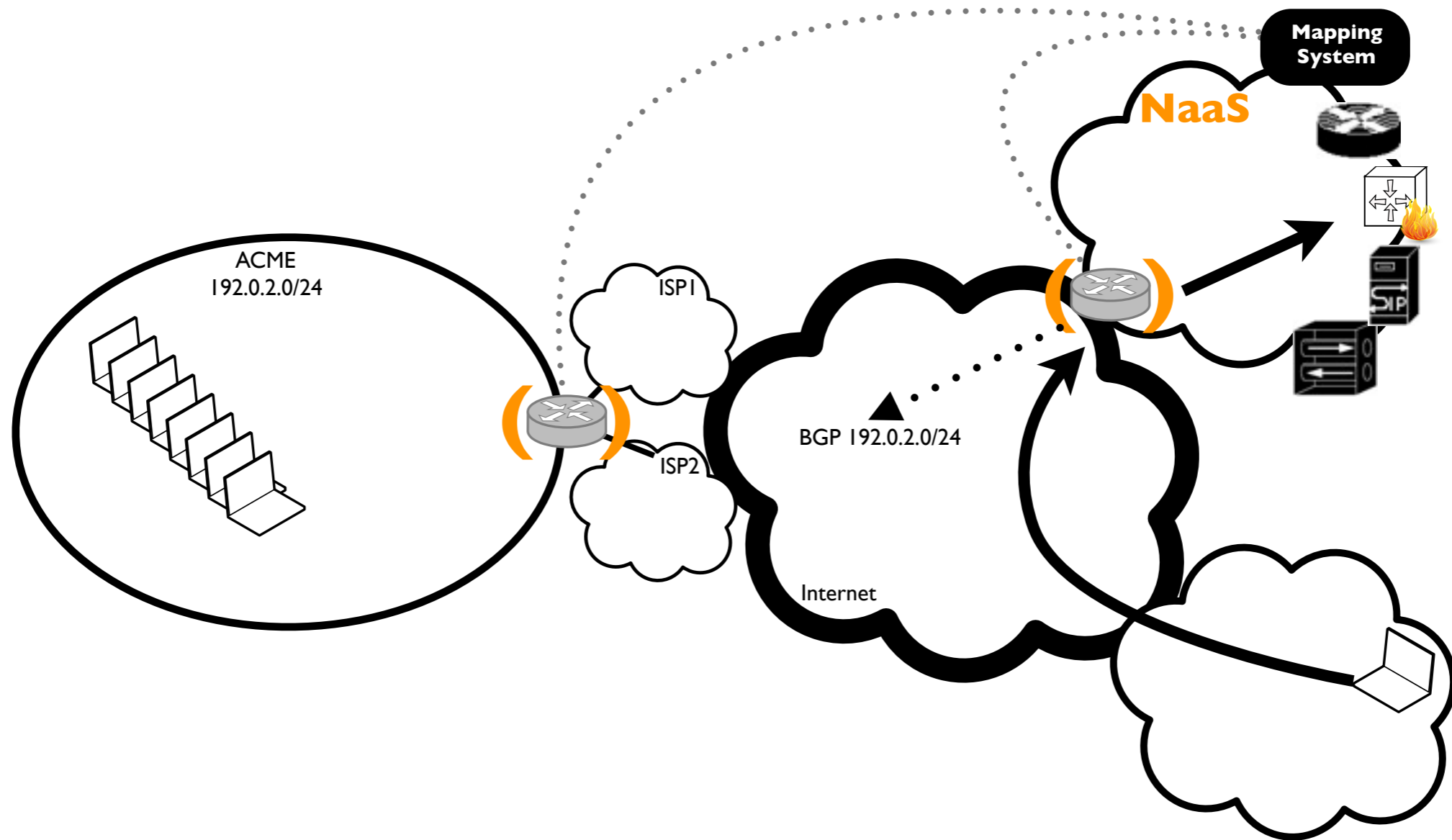
- Native IP forwarding
- ⋯▶ BGP advertisement
- - - → LISP tunnel
- || (router icon) LISP router

From the Internet



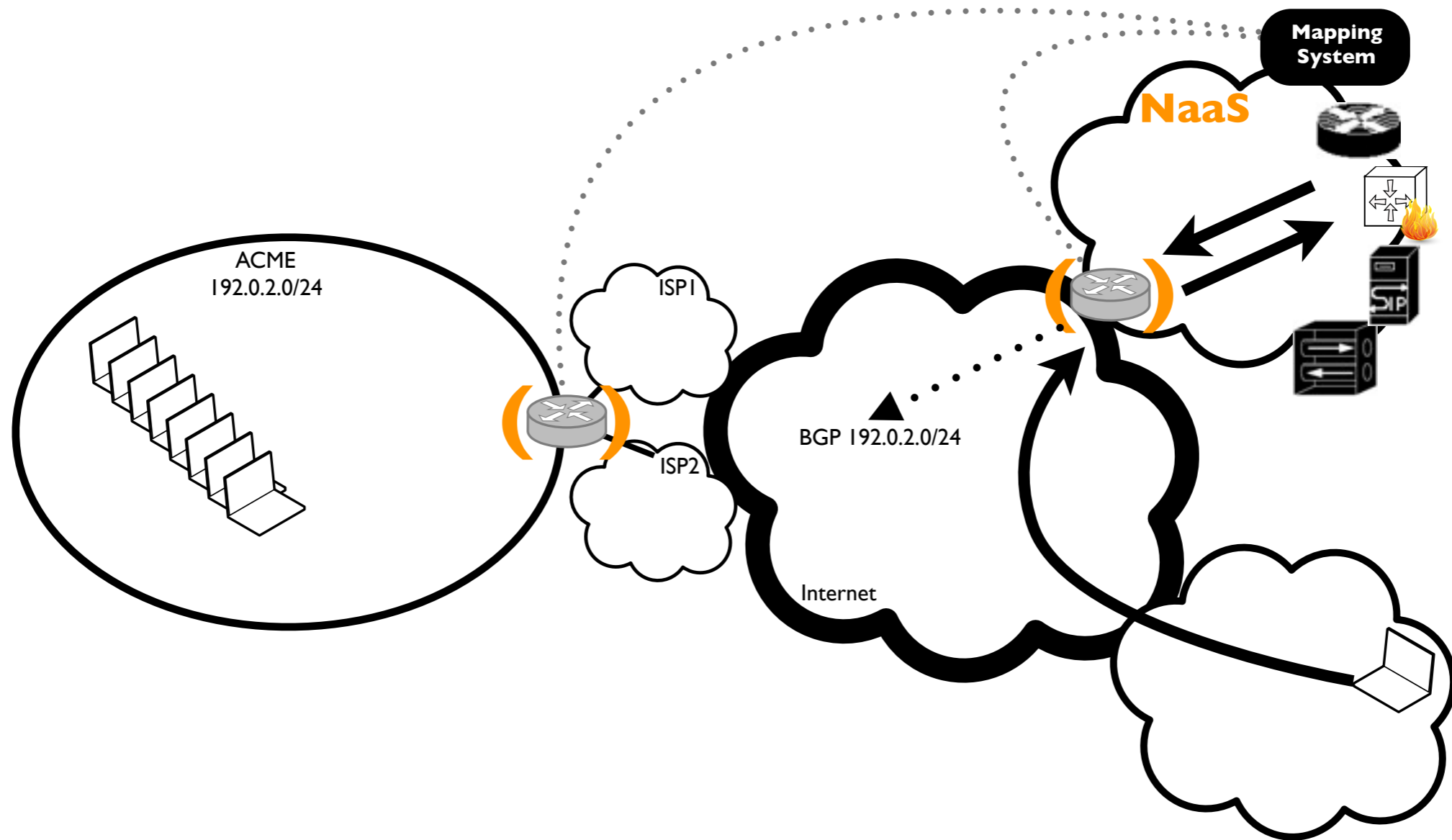
————→ Native IP forwarding ▶ BGP advertisement
○- - - - -▶ LISP tunnel || (router) LISP router

From the Internet



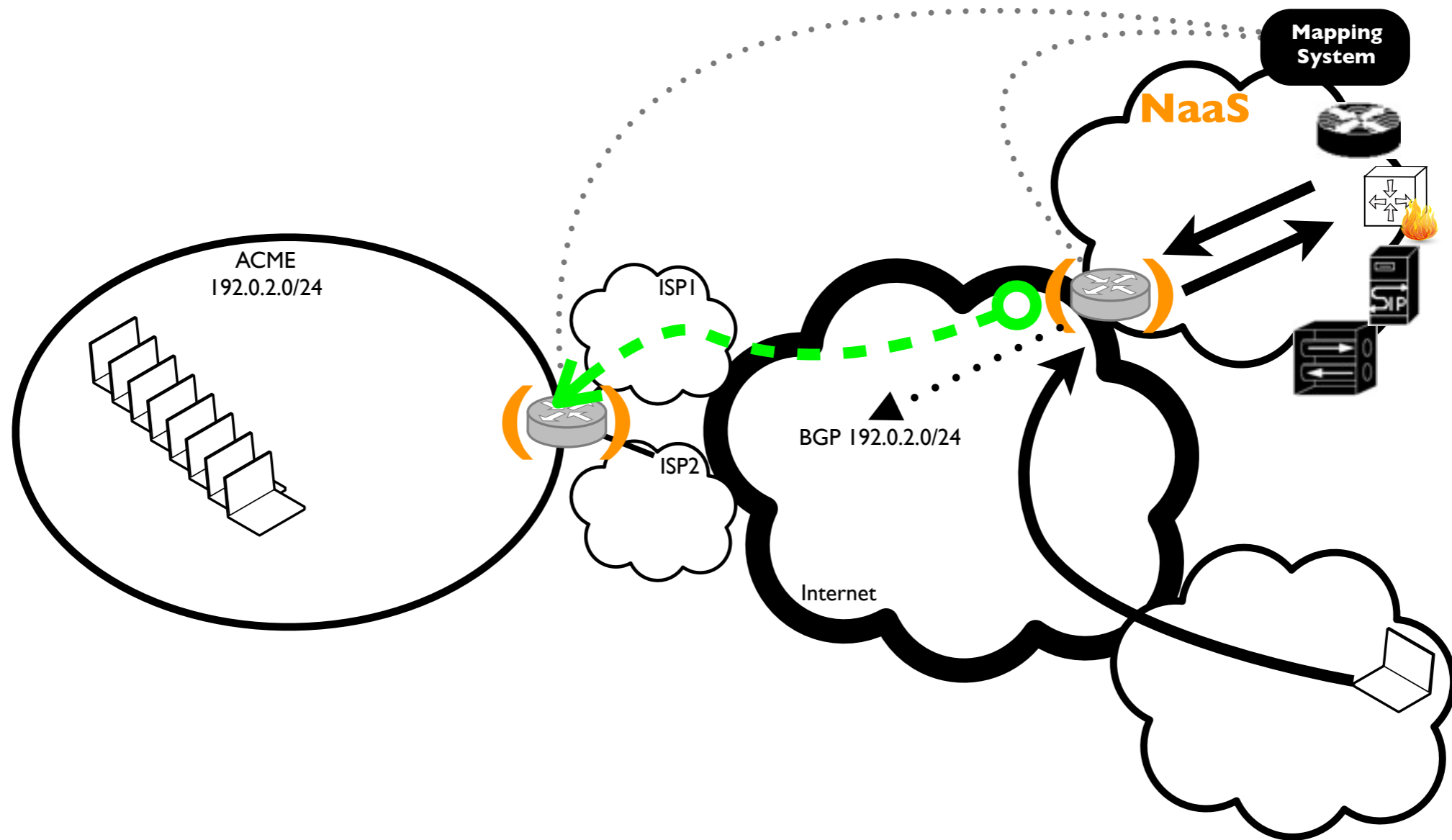
- Native IP forwarding
- ⋯ BGP advertisement
- - - → LISP tunnel
- || (router icon) LISP router

From the Internet

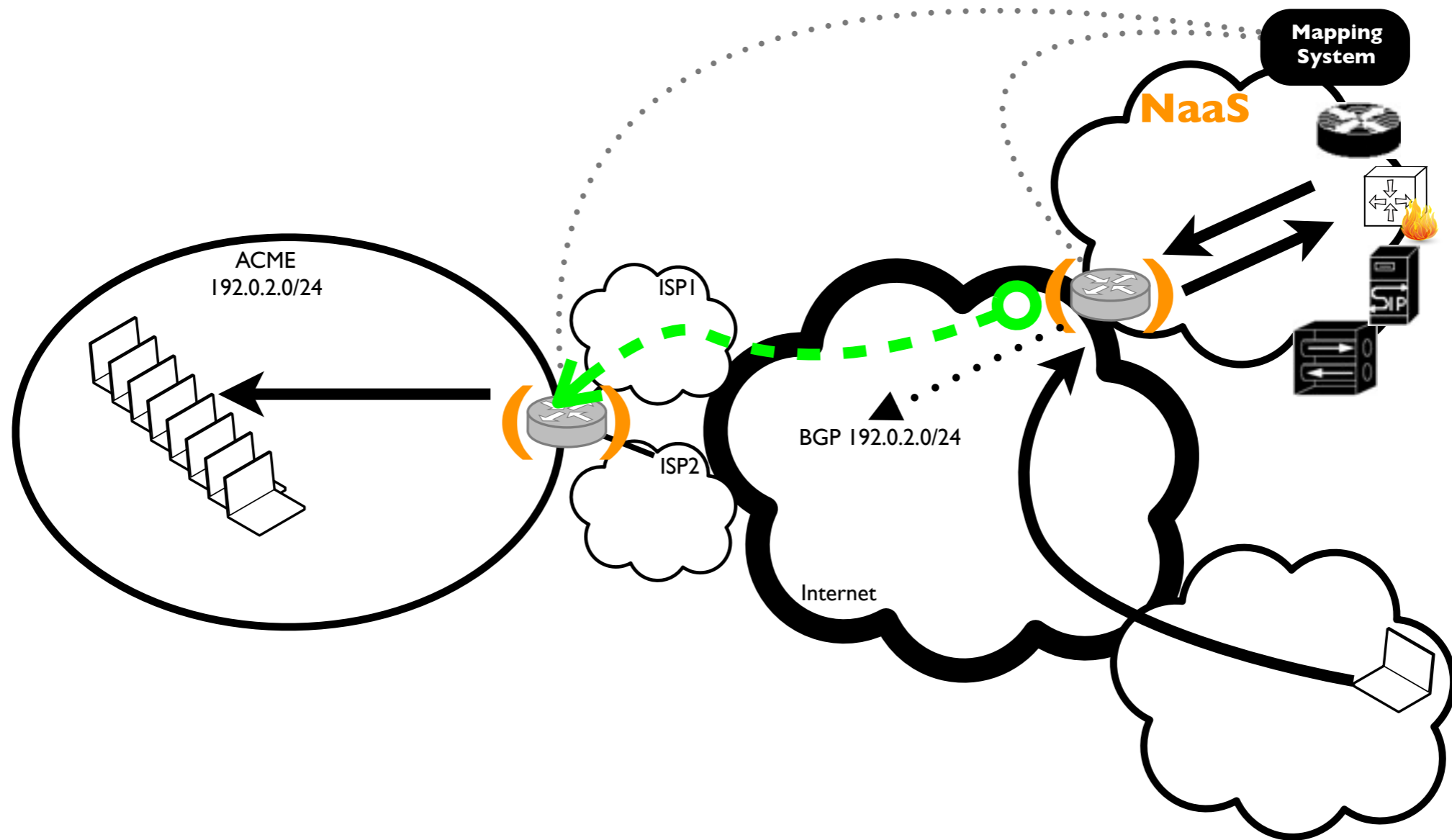


- Native IP forwarding
- ⋯ BGP advertisement
- - - → LISP tunnel
- ||
- (Router icon) LISP router

From the Internet



From the Internet



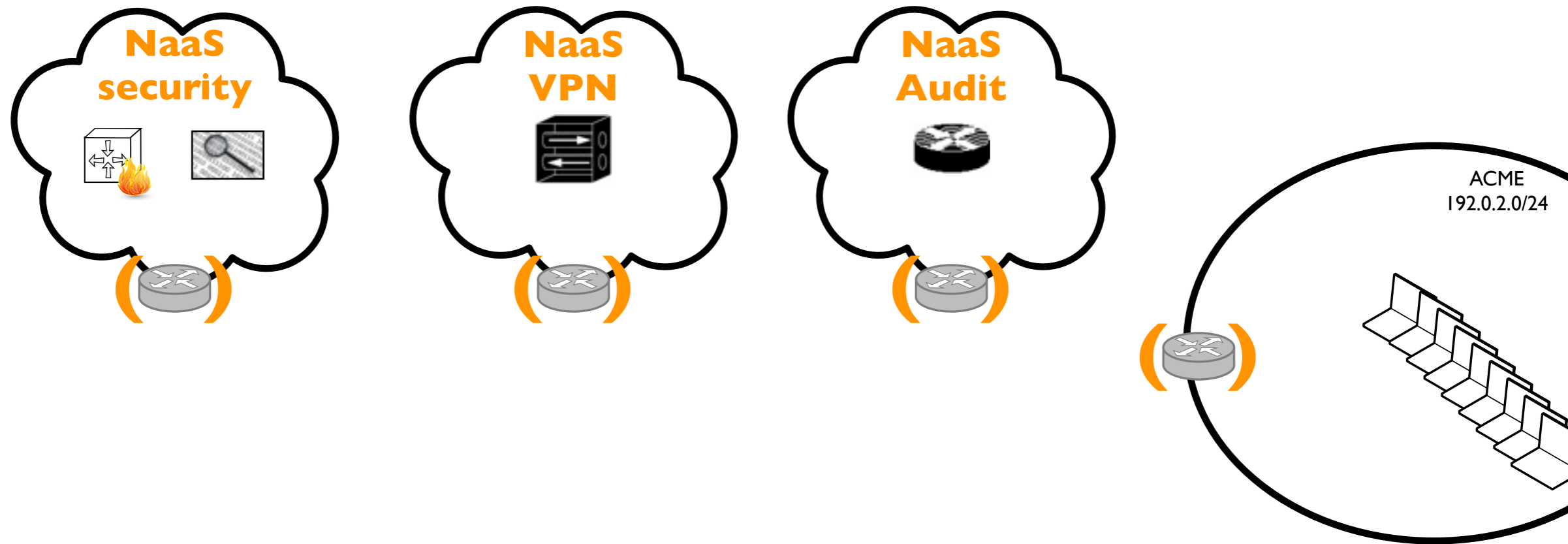
————→ Native IP forwarding

○- - - -> LISP tunnel

.....▶ BGP advertisement

(Router) LISP router

NaaS Chaining

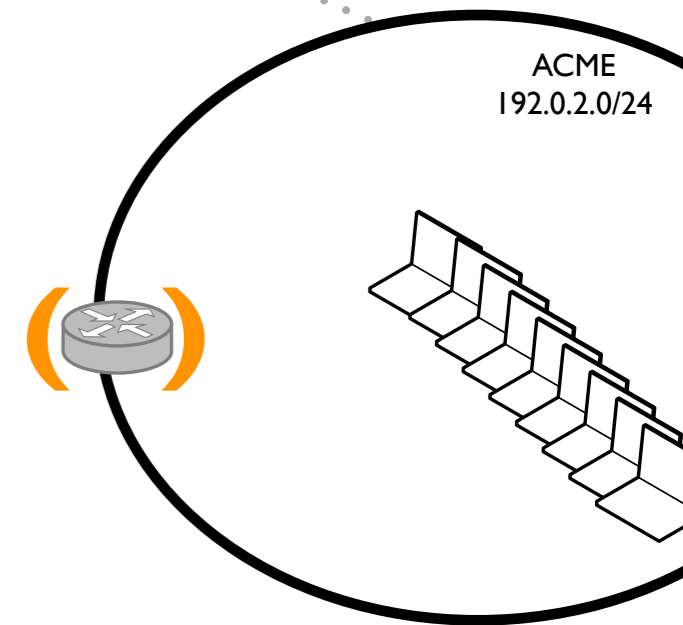
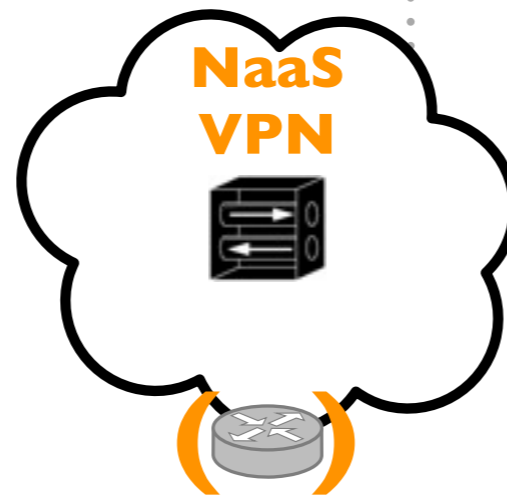
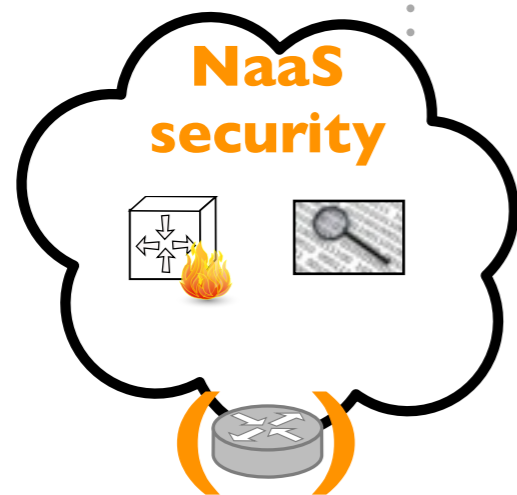


○ - ➔ LISP tunnel (Router) LISP router

•• ▶ BGP advertisement ➔ Native IP forwarding

NaaS Chaining

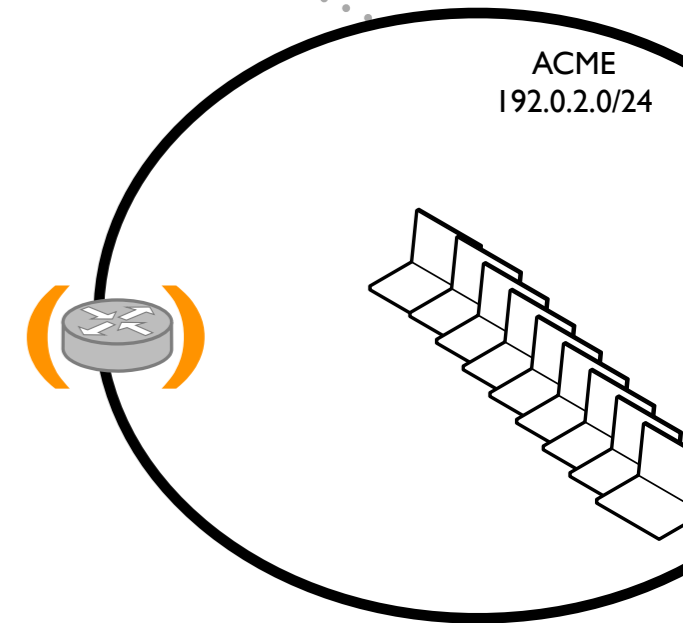
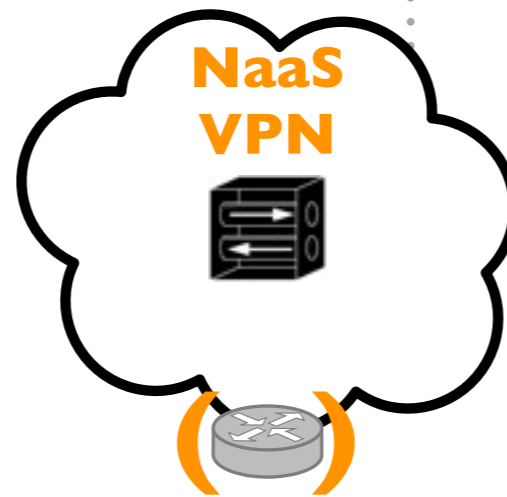
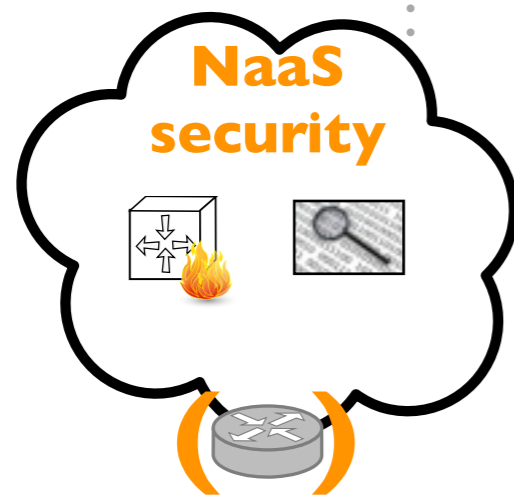
Order	NaaS	Operation
1	Security	firewall
2	VPN	VPN
3	Audit	Netflow
4	Security	deep packet inspection



○ - ➔ LISP tunnel
 LISP router
 ⋯ ▶ BGP advertisement
 ➔ Native IP forwarding

NaaS Chaining

Order	NaaS	Operation	Input	Output
1	Security	firewall	<u>native</u>	instance-id: 0x1
2	VPN	VPN	instance-id: 0x1	instance-id: 0x2
3	Audit	Netflow	instance-id: 0x2	instance-id: 0x3
4	Security	deep packet inspection	instance-id: 0x3	instance-id: 0x4



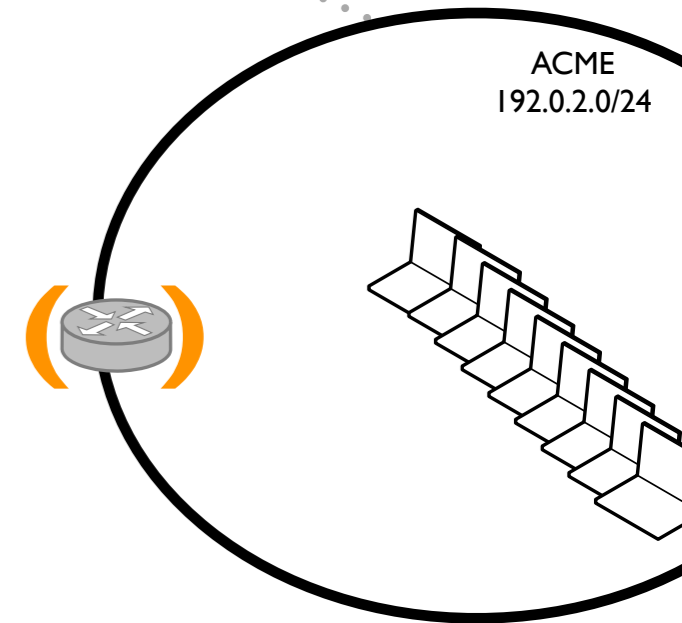
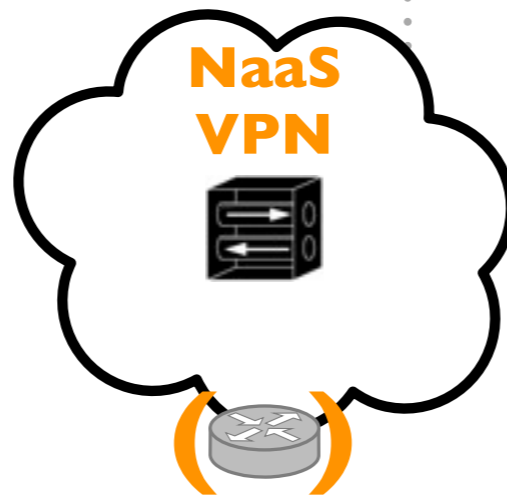
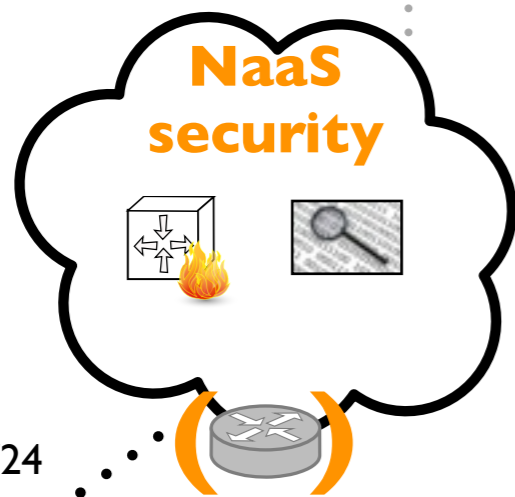
○ - ➔ LISP tunnel

(Router icon) LISP router

⋯ ▶ BGP advertisement ➔ Native IP forwarding

NaaS Chaining

Order	NaaS	Operation	Input	Output
1	Security	firewall	<u>native</u>	instance-id: 0x1
2	VPN	VPN	instance-id: 0x1	instance-id: 0x2
3	Audit	Netflow	instance-id: 0x2	instance-id: 0x3
4	Security	deep packet inspection	instance-id: 0x3	instance-id: 0x4

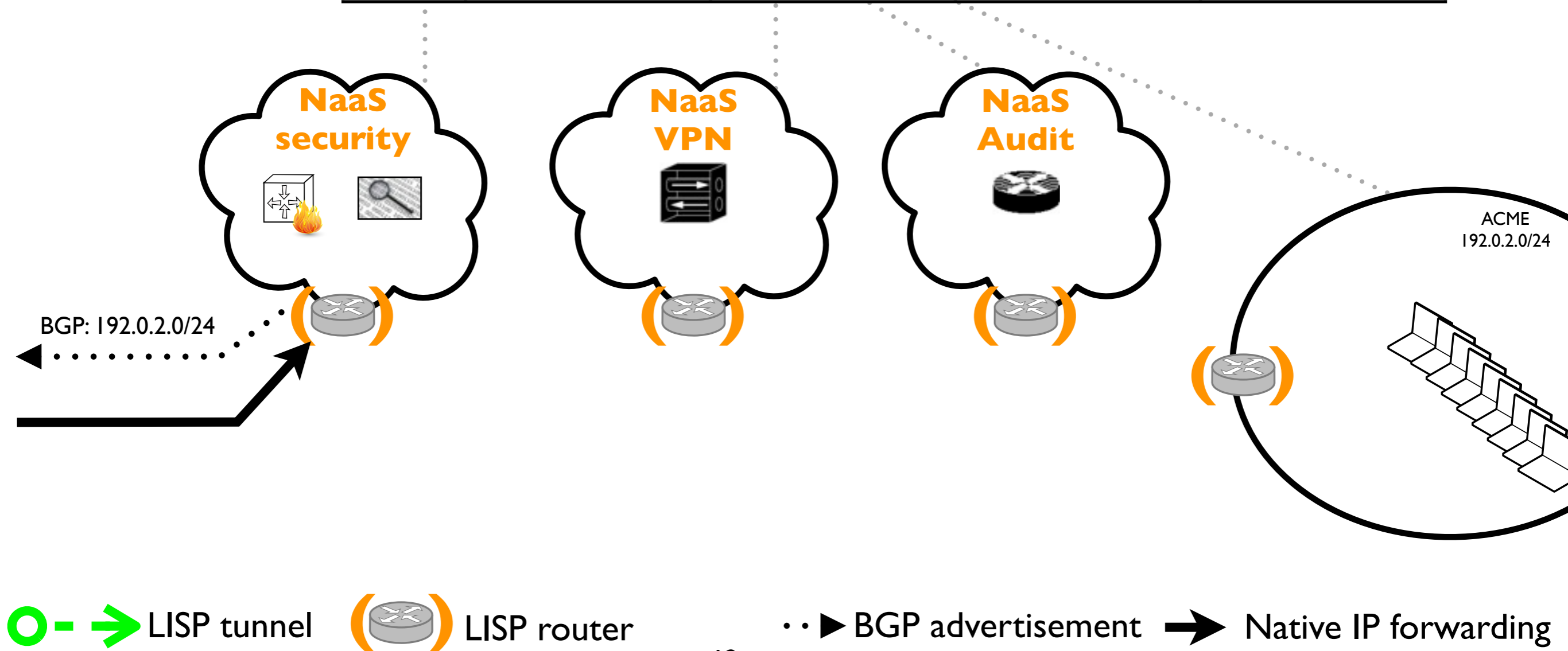


BGP: 192.0.2.0/24

○ - ➔ LISP tunnel
 LISP router
 ⋯ ➤ BGP advertisement
 ➔ Native IP forwarding

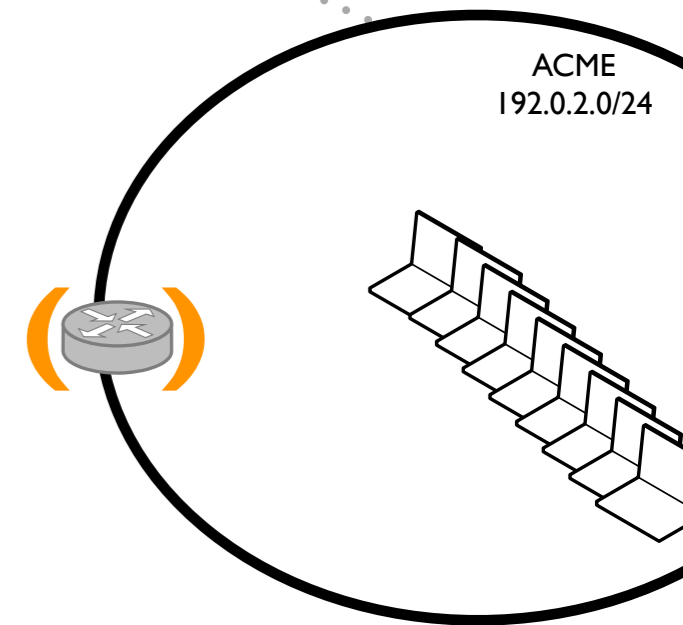
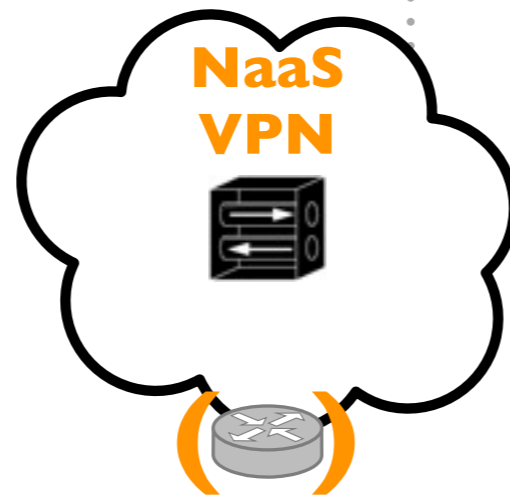
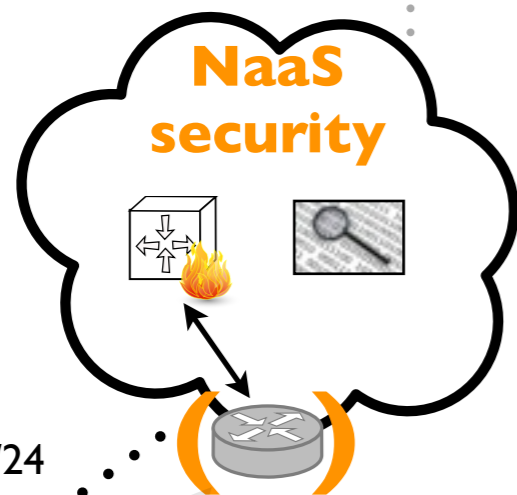
NaaS Chaining

Order	NaaS	Operation	Input	Output
1	Security	firewall	<u>native</u>	instance-id: 0x1
2	VPN	VPN	instance-id: 0x1	instance-id: 0x2
3	Audit	Netflow	instance-id: 0x2	instance-id: 0x3
4	Security	deep packet inspection	instance-id: 0x3	instance-id: 0x4



NaaS Chaining

Order	NaaS	Operation	Input	Output
1	Security	firewall	<u>native</u>	instance-id: 0x1
2	VPN	VPN	instance-id: 0x1	instance-id: 0x2
3	Audit	Netflow	instance-id: 0x2	instance-id: 0x3
4	Security	deep packet inspection	instance-id: 0x3	instance-id: 0x4

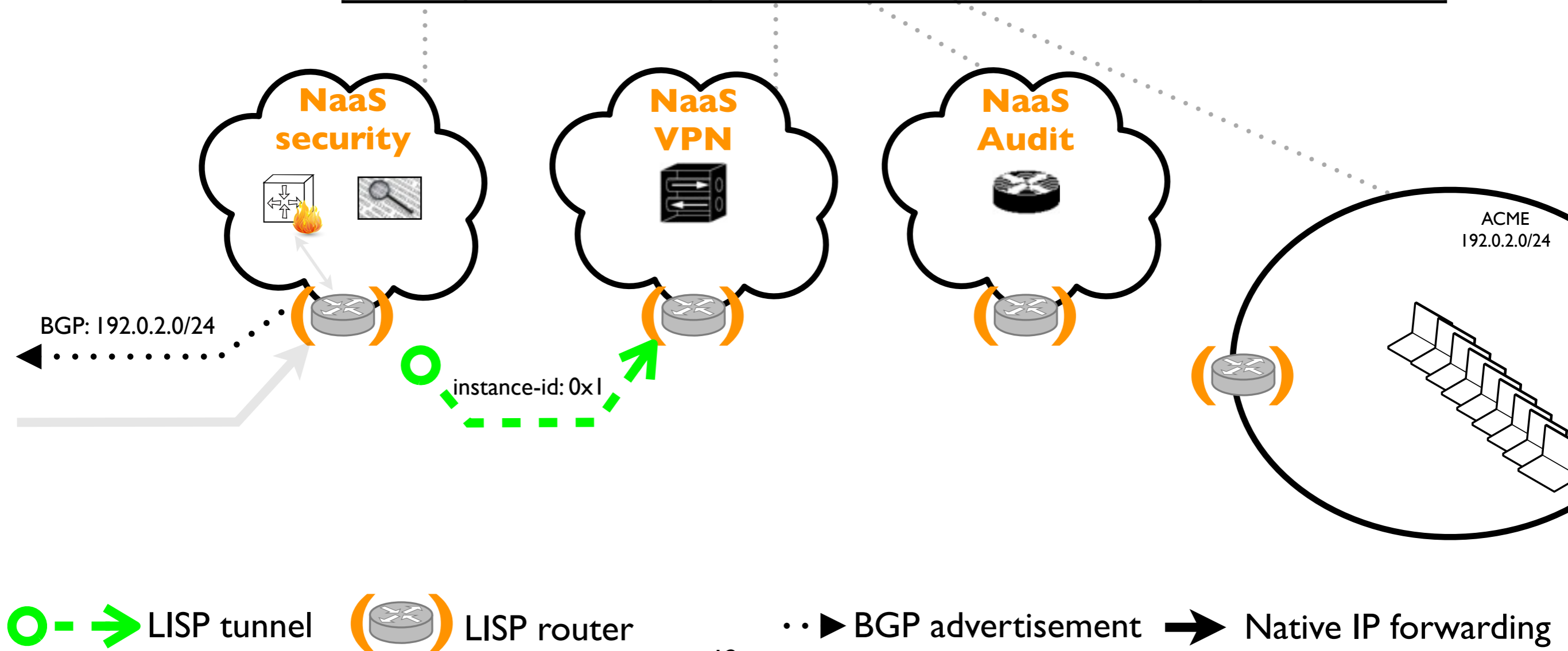


BGP: 192.0.2.0/24

○ - ➔ LISP tunnel
 LISP router
 ⋯ ➤ BGP advertisement
 ➔ Native IP forwarding

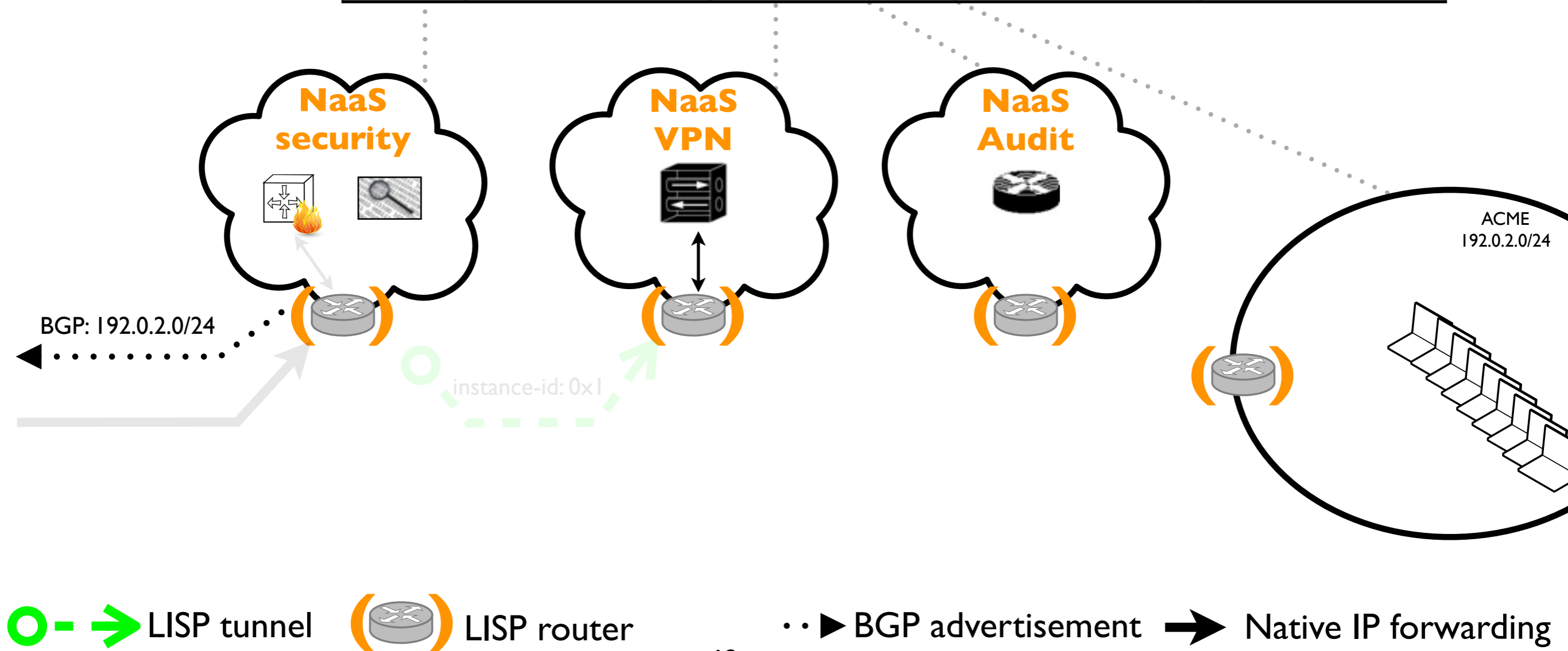
NaaS Chaining

Order	NaaS	Operation	Input	Output
1	Security	firewall	<u>native</u>	instance-id: 0x1
2	VPN	VPN	instance-id: 0x1	instance-id: 0x2
3	Audit	Netflow	instance-id: 0x2	instance-id: 0x3
4	Security	deep packet inspection	instance-id: 0x3	instance-id: 0x4



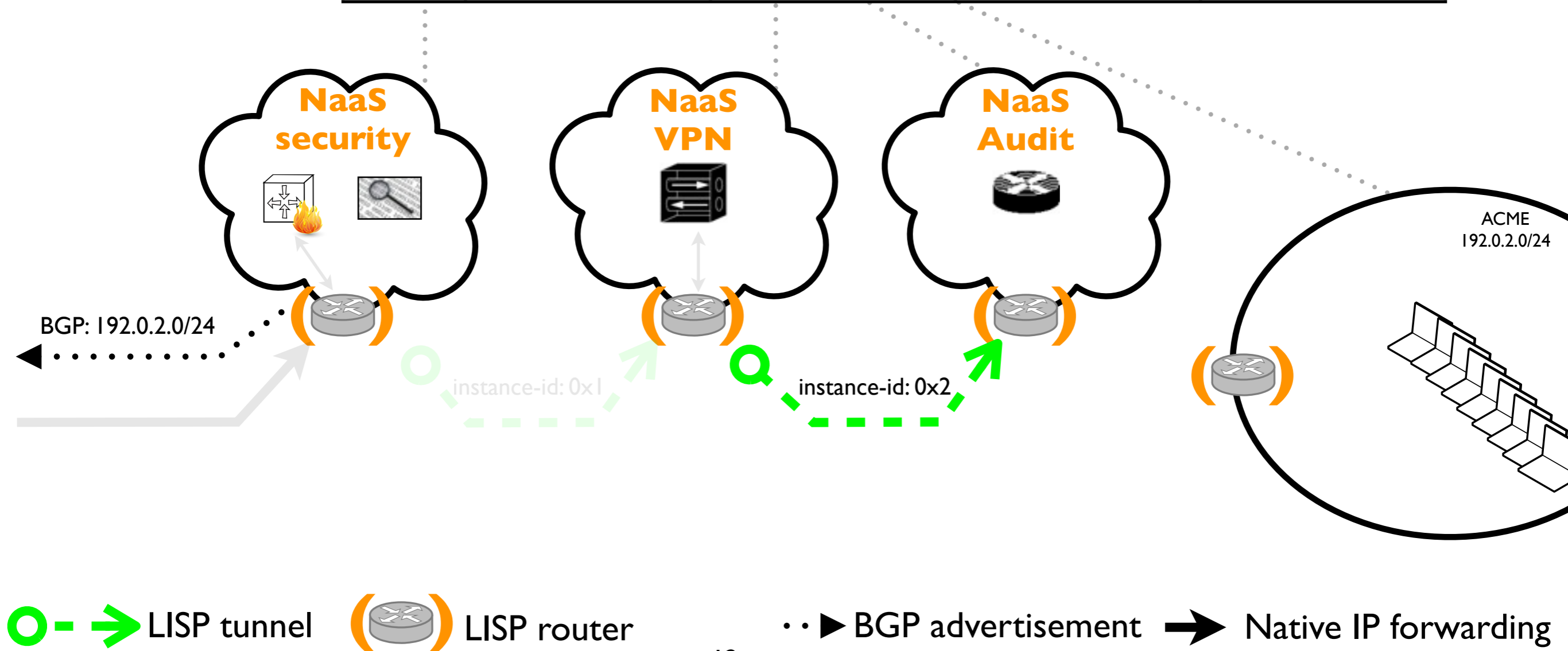
NaaS Chaining

Order	NaaS	Operation	Input	Output
1	Security	firewall	<u>native</u>	instance-id: 0x1
2	VPN	VPN	instance-id: 0x1	instance-id: 0x2
3	Audit	Netflow	instance-id: 0x2	instance-id: 0x3
4	Security	deep packet inspection	instance-id: 0x3	instance-id: 0x4



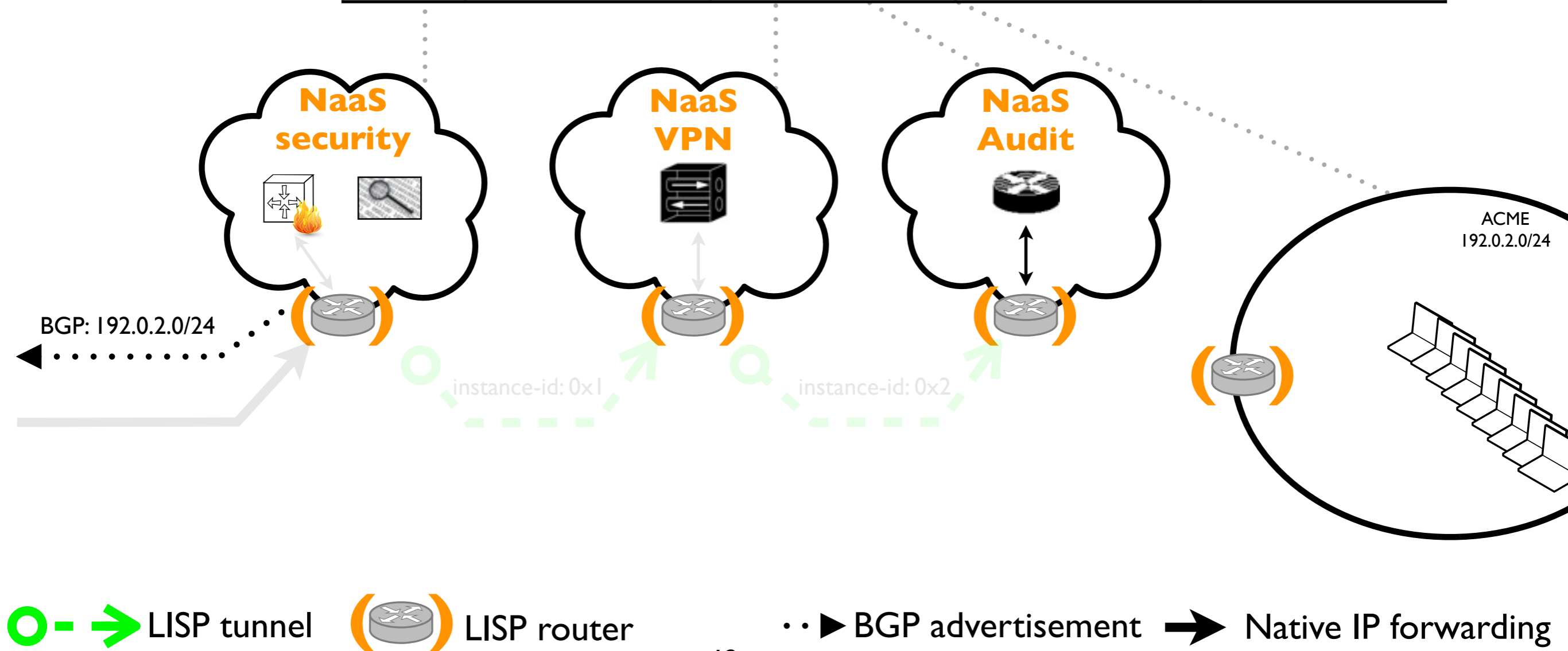
NaaS Chaining

Order	NaaS	Operation	Input	Output
1	Security	firewall	<u>native</u>	instance-id: 0x1
2	VPN	VPN	instance-id: 0x1	instance-id: 0x2
3	Audit	Netflow	instance-id: 0x2	instance-id: 0x3
4	Security	deep packet inspection	instance-id: 0x3	instance-id: 0x4



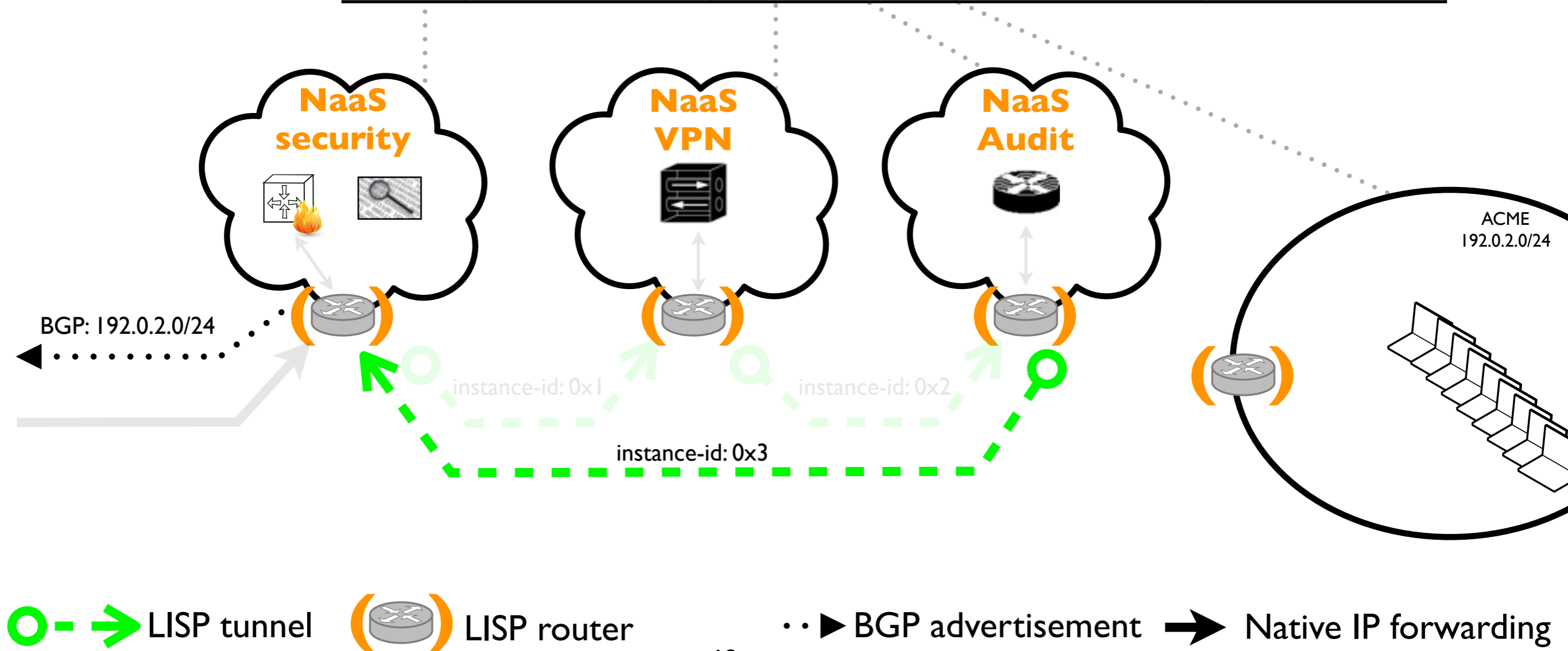
NaaS Chaining

Order	NaaS	Operation	Input	Output
1	Security	firewall	<u>native</u>	instance-id: 0x1
2	VPN	VPN	instance-id: 0x1	instance-id: 0x2
3	Audit	Netflow	instance-id: 0x2	instance-id: 0x3
4	Security	deep packet inspection	instance-id: 0x3	instance-id: 0x4



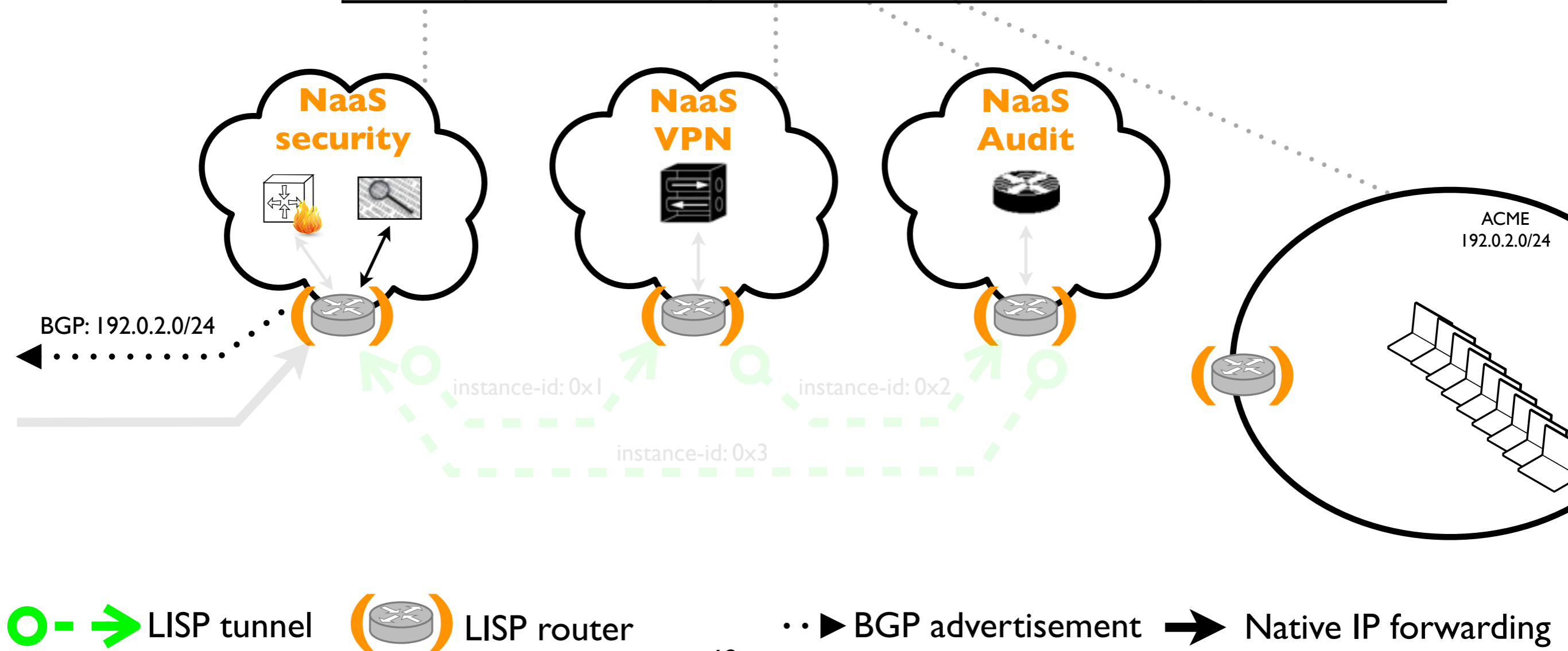
NaaS Chaining

Order	NaaS	Operation	Input	Output
1	Security	firewall	<u>native</u>	instance-id: 0x1
2	VPN	VPN	instance-id: 0x1	instance-id: 0x2
3	Audit	Netflow	instance-id: 0x2	instance-id: 0x3
4	Security	deep packet inspection	instance-id: 0x3	instance-id: 0x4



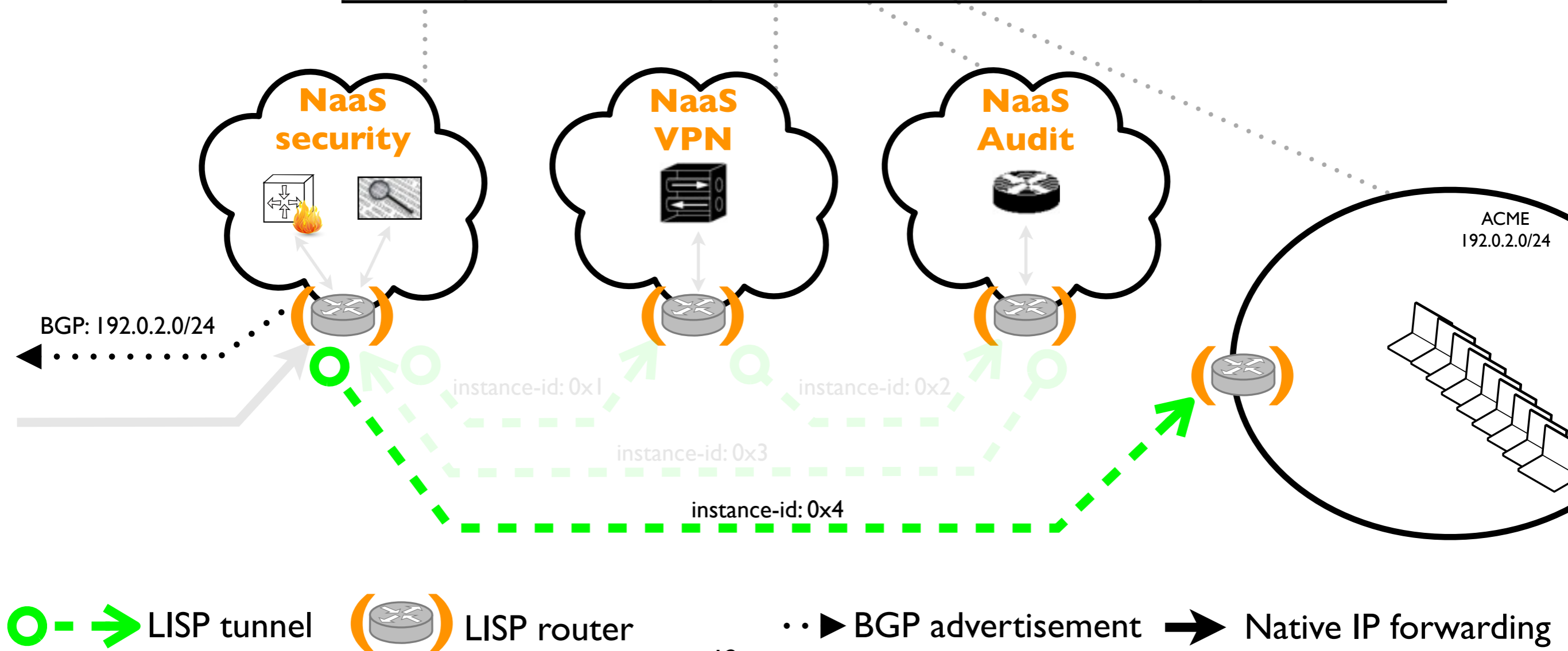
NaaS Chaining

Order	NaaS	Operation	Input	Output
1	Security	firewall	<u>native</u>	instance-id: 0x1
2	VPN	VPN	instance-id: 0x1	instance-id: 0x2
3	Audit	Netflow	instance-id: 0x2	instance-id: 0x3
4	Security	deep packet inspection	instance-id: 0x3	instance-id: 0x4



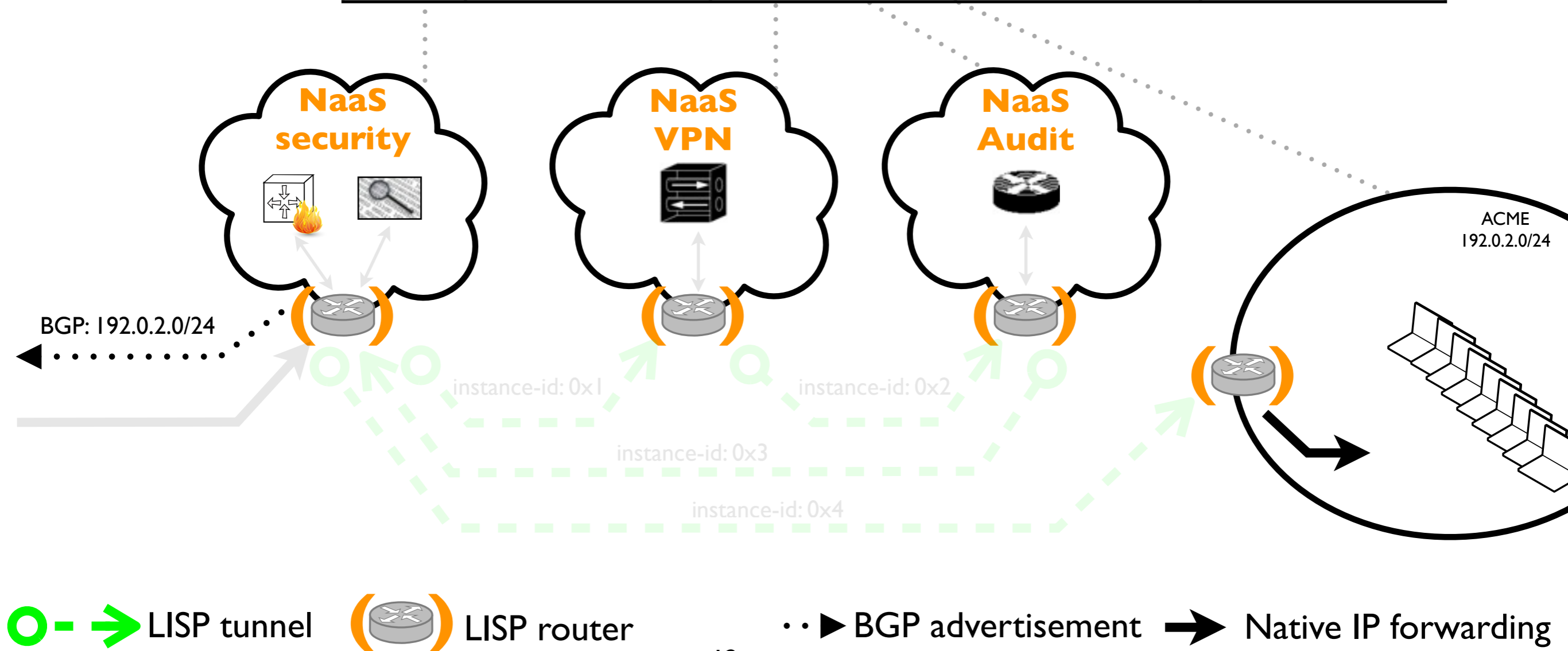
NaaS Chaining

Order	NaaS	Operation	Input	Output
1	Security	firewall	<u>native</u>	instance-id: 0x1
2	VPN	VPN	instance-id: 0x1	instance-id: 0x2
3	Audit	Netflow	instance-id: 0x2	instance-id: 0x3
4	Security	deep packet inspection	instance-id: 0x3	instance-id: 0x4



NaaS Chaining

Order	NaaS	Operation	Input	Output
1	Security	firewall	<u>native</u>	instance-id: 0x1
2	VPN	VPN	instance-id: 0x1	instance-id: 0x2
3	Audit	Netflow	instance-id: 0x2	instance-id: 0x3
4	Security	deep packet inspection	instance-id: 0x3	instance-id: 0x4



Summary

- Maintaining fast, secure, and reliable Internet connectivity is expensive for enterprises
- Moving network infrastructure to the Cloud (i.e., Network-as-a-Service) reduces costs
- LISP is an enabler for NaaS

Network in the Cloud: a Map-and-Encap Approach

Damien Saucez

Inria

Wassim Haddad

Ericsson

IEEE CloudNet'12

Backup

Outsourcing

- Outsource: “*obtain (goods or a service) by contract from an outside supplier*” [20]
- Network management is often outsourced to external enterprises to reduce OPEX
 - but devices still have to be deployed locally
- High level services (e.g., web server, emails) are frequently outsourced to the Cloud
 - but low-level services (e.g., firewall, IDS) are not